FUJITSU

# Integrated Lights Out Manager 2.0 Benutzerhandbuch

Handbuch-Code: C120-E474-01DE
Teile-Nr. 875-4285-10
Oktober 2007, Revision A

Copyright 2007 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, Kalifornien 95054, USA. Alle Rechte vorbehalten.

Sun Microsystems, Inc., besitzt die geistigen Eigentumsrechte an der in diesem Dokument beschriebenen Technologie. Insbesondere und ohne Einschränkung können die geistigen Eigentumsrechte ein oder mehrere der US-Patente umfassen, die unter http://www.sun.com/patents aufgelistet sind, sowie ein oder mehrere zusätzliche Patente bzw. laufende Patentanmeldungen in den USA und in anderen Ländern.

Dieses Dokument und das zugehörige Produkt werden unter Lizenzen vertrieben, die seine Verwendung, Vervielfältigung, Weitergabe und Dekompilierung eingeschränken. Ohne vorherige schriftliche Genehmigung von Sun und gegebenenfalls seiner Lizenzgeber darf dieses Produkt oder Dokument weder ganz noch auszugsweise in irgendeiner Form oder mit irgendwelchen Mitteln reproduziert werden.

Die Software von Fremdherstellern, einschließlich der Schriftentechnologie, ist urheberrechtlich geschützt und wird von Sun-Lieferanten lizenziert.

Teile dieses Produkts können auf Berkeley BSD-Systemen basieren, die von der University of California lizenziert werden. UNIX ist in den USA und in anderen Ländern eine eingetragene Marke, die ausschließlich durch X/Open Company, Ltd., lizenziert wird.

Sun, Sun Microsystems, das Sun-Logo, Java, docs.sun.com und Solaris sind Marken oder eingetragene Marken von Sun Microsystems, Inc., in den USA und anderen Ländern.

Alle SPARC-Marken werden unter Lizenz verwendet und sind Marken oder eingetragene Marken von SPARC International, Inc., in den USA und in anderen Ländern. Produkte, die SPARC-Marken tragen, basieren auf einer von Sun Microsystems, Inc., entwickelten Architektur.

OPEN LOOK und die grafische Benutzeroberfläche von Sun™ wurden von Sun Microsystems, Inc., für seine Benutzer und Lizenznehmer entwickelt. Sun anerkennt dabei die von Xerox geleistete Forschungs- und Entwicklungsarbeit auf dem Gebiet der visuellen und grafischen Benutzeroberflächen für die Computerindustrie. Sun ist Inhaber einer nicht ausschließlichen Lizenz von Xerox für die grafische Benutzeroberfläche von Xerox. Diese Lizenz gilt auch für die Lizenznehmer von Sun, die mit den OPEN LOOK-Spezifikationen übereinstimmende Benutzerschnittstellen implementieren und sich an die schriftlichen Lizenzvereinbarungen mit Sun halten.

DIE DOKUMENTATION WIRD IN DER VORLIEGENDEN FORM GELIEFERT UND ALLE AUSDRÜCKLICHEN ODER IMPLIZITEN BEDINGUNGEN, ZUSICHERUNGEN UND GEWÄHRLEISTUNGEN, EINSCHLIESSLICH JEGLICHER IMPLIZITEN GEWÄHRLEISTUNG HINSICHTLICH HANDELSÜBLICHER QUALITÄT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER WAHRUNG DER RECHTE DRITTER, WERDEN AUSGESCHLOSSEN, SOWEIT EIN SOLCHER HAFTUNGSAUSSCHLUSS GESETZLICH ZULÄSSIG IST.

Bitte
Wiederverwenden

Adobe PostScript

# Inhalt

**Vorwort xvii**

**1. Einführung in ILOM 1**

Was ist ILOM? 1

ILOM auf SP und CMM 2

ILOM-Schnittstellen 3

ILOM-Verwaltungsnetzwerk 4

ILOM-Verbindungsmethoden 5

Rollen für ILOM-Benutzerkonten 6

Vorkonfiguriertes ILOM-Administratorkonto 6

ILOM-Leistungsmerkmale 7

Neue Leistungsmerkmale in ILOM 2.0 9

**2. Herstellen der ersten Kommunikation mit ILOM 11**

Erste ILOM-Einrichtung 12

Arbeitsblatt für die erste Einrichtung 12

Aspekte bei der IP-Zuweisung über DHCP 15

Senden des DHCPDISCOVER-Pakets auf Serverplattformen 15

Voraussetzungen für die Zuweisung über DHCP 15

MAC-Adresse der SP-Netzwerkschnittstelle 16

Anforderungen nach der Zuweisung über DHCP 17

Aspekte bei der Zuweisung statischer IPs 18

Voraussetzungen für die Zuweisung statischer IP-Adressen 18

Einstellungen des seriellen Geräts bzw. der Terminalemulationssoftware 19

Nach der Zuweisung statischer IP-Adressen 19

Konfiguration von Verwaltungsnetzwerk-IP-Adressen 20

Zuweisen von ILOM-Netzwerkanschlüssen 20

Hostnamenkennung für Server-SP und CMM 22

Systemkennungs-Textzeichenfolgen für Server 22

Zuweisen von IP-Adressen zu den Serverplattform-SP-Schnittstellen 23

- Zuweisen von IP-Adressen über DHCP mithilfe einer Ethernet-Verwaltungsverbindung 23
- Zuweisen einer statischen IP-Adresse zum Server-SP mithilfe einer seriellen Verbindung 25
- Zuweisen einer statischen IP-Adresse zum CMM mithilfe einer seriellen Verbindung 27

Bearbeiten von IP-Adressenzuweisungen mithilfe einer Ethernet-Verwaltungsverbindung 29

- Bearbeiten vorhandener IP-Adressen in ILOM mithilfe der Webbenutzeroberfläche 29
- Bearbeiten vorhandener IP-Adressen in ILOM mithilfe der CLI 31

Zuweisen von Hostnamen oder Systemkennungen 33

- Zuweisen von Hostnamen oder Systemkennungen mithilfe der Webbenutzeroberfläche 33
- Zuweisen von Hostnamen oder Systemkennungen mithilfe der CLI 34

**3. ILOM-Befehlszeilenschnittstelle (CLI) und Anmeldung 37**

CLI – Überblick 38

Hierarchische CLI-Architektur 38

CLI-Befehlssyntax 40

CLI-Befehle 40

Befehlsoptionen 41

Befehlsziele 41

Befehlseigenschaften 41

Befehlsausführung 42

- Ausführen einzelner Befehle 42
- Ausführen kombinierter Befehle 42

Herstellen einer Verbindung mit ILOM mithilfe der CLI 43

- Anmelden bei ILOM 43
- Abmelden von ILOM 44

**4. ILOM-Webbenutzeroberfläche und Anmeldung 45**

Webbenutzeroberfläche – Überblick 45

Anforderungen an Browser und Software 46

Komponenten der Webbenutzeroberfläche 47

Komponenten der Navigationsregisterkarten 48

Registerkarte System Information 49

Registerkarte Versions 49

Registerkarte Session Time-Out 49

Registerkarte Components 49

Registerkarte Identification Information 50

Registerkarte System Monitoring 50

Registerkarte Sensor Readings 50

Registerkarte Indicators 50

Registerkarte Event Logs 51

Registerkarte Configuration 51

Registerkarte System Management Access 51

Registerkarte Alert Management 52

Registerkarte Network 52

Registerkarte Serial Port 53

Registerkarte Clock Settings 53

Registerkarte Syslog 53
Registerkarte SMTP Client 53
Registerkarte Policy 53
Registerkarte User Management 54
Registerkarte User Accounts 54
Registerkarte Active Sessions 54
Registerkarte LDAP 54
Registerkarte RADIUS 55
Registerkarte Active Directory 55
Registerkarte Remote Control 55
Registerkarte Redirection 55
Registerkarte Remote Power Control 56
Registerkarte Mouse Mode Settings 56
Registerkarte Maintenance 56
Registerkarte Firmware Upgrade 57
Registerkarte Reset SP 57
Herstellen einer Verbindung mit ILOM mithilfe der Webbenutzeroberfläche 57
- Anmelden bei ILOM 57
- Hochladen des SSL-Zertifikats 60
- Festlegen der Sitzungszeitüberschreitung 61
- Abmelden von ILOM 62

**5. Verwalten von Benutzerkonten 63**

Richtlinien für die Verwaltung von Benutzerkonten 65
Benutzerkontenrollen und -berechtigungen 65
Vorkonfigurierte ILOM-Administratorkonten 66
- Ändern des Passworts des root-Kontos in ILOM mithilfe der Webbenutzeroberfläche 66
- Ändern des Passworts des root-Kontos in ILOM mithilfe der CLI 69

Single Sign On 69

- Aktivieren und Deaktivieren von Single Sign On mithilfe der CLI 69
- Aktivieren und Deaktivieren von Single Sign On mithilfe der Webbenutzeroberfläche 70

Verwalten von Benutzerkonten mithilfe der CLI 70

- Hinzufügen eines Benutzerkontos mithilfe der CLI 71
- Ändern eines Benutzerkontos mithilfe der CLI 71
- Löschen eines Benutzerkontos mithilfe der CLI 71
- Anzeigen einer Liste von Benutzerkonten mithilfe der CLI 71
- Anzeigen eines einzelnen Benutzerkontos mithilfe der CLI 72
- Konfigurieren eines Benutzerkontos mithilfe der CLI 72

  Ziele, Eigenschaften und Werte 73
- Anzeigen einer Liste von Benutzersitzungen mithilfe der CLI 73
- Anzeigen einer einzelnen Benutzersitzung mithilfe der CLI 74

Verwalten von Benutzerkonten mithilfe der Webbenutzeroberfläche 74

- Hinzufügen von Benutzerkonten und Festlegen von Berechtigungen mithilfe der Webbenutzeroberfläche 74
- Ändern eines Benutzerkontos mithilfe der Webbenutzeroberfläche 77
- Löschen eines Benutzerkontos mithilfe der Webbenutzeroberfläche 80
- Anzeigen von Benutzersitzungen mithilfe der Webbenutzeroberfläche 81

Active Directory 82

Informationen zu Active Directory 82

Konfigurieren von Active Directory 83

- Konfigurieren von Active Directory mithilfe der Webbenutzeroberfläche 83

  Eigenschaften der Seite Active Directory-Konfiguration 84

  Active Directory-Zieltabellen 85

  Eigenschaften von Active Directory-Zieltabellen 87

- Bearbeiten von Active Directory-Tabelleninformationen mithilfe der Webbenutzeroberfläche 88

Ermitteln der Benutzerautorisierungsstufe 89

Absichern der Active Directory-Verbindung 90

Absichern der Active Directory-Verbindung mithilfe der CLI 90

- Ausführen von Aktionen mit `getcertfile` mithilfe der CLI 90
- Aktivieren von `strictcertmode` mithilfe der CLI 91
- Prüfen des `certfilestatus` mithilfe der CLI 91

Absichern der Active Directory-Verbindung mithilfe der Webbenutzeroberfläche 92

- Hochladen eines Zertifikats mithilfe der Webbenutzeroberfläche 92
- Prüfen des Status der Zertifikatdatei mithilfe der Webbenutzeroberfläche 93
- Aktivieren des Strict Certificate Mode mithilfe der Webbenutzeroberfläche 93

LDAP (Lightweight Directory Access Protocol) 94

Informationen zu LDAP 94

LDAP-Clients und -Server 94

Verzeichnisorganisation auf LDAP-Servern 95

Konfigurieren von LDAP 96

- Konfigurieren des LDAP-Servers 97
- Konfigurieren von ILOM für LDAP mithilfe der CLI 98
- Konfigurieren von ILOM für LDAP mithilfe der Webbenutzeroberfläche 99

RADIUS-Authentifizierung 100

RADIUS-Clients und -Server 100

RADIUS-Parameter 101

Konfigurieren von RADIUS-Einstellungen 101

- Konfigurieren von RADIUS mithilfe der CLI 102
- Konfigurieren von RADIUS mithilfe der Webbenutzeroberfläche 102

RADIUS-Befehle 103

`show /SP/clients/radius` 103

`set /SP/clients/radius` 104

`show /SP/clients` 105

**6. Bestands- und Komponentenverwaltung 107**

Anzeigen von Komponenteninformationen und Verwalten des Bestands 108

- Anzeigen von Komponenteninformationen mithilfe der CLI 108
- Anzeigen von Komponenteninformationen mithilfe der Webbenutzeroberfläche 109

Ausführen einer Aktion mit einer Komponente 110

Entfernen und Austauschen von Komponenten 111

- Vorbereiten des Entfernens einer Komponente mithilfe der CLI 111
- Ermitteln der Bereitschaft einer Komponente zum Entfernen mithilfe der CLI 111
- Wiederinbetriebnehmen einer Komponente mithilfe der CLI 112
- Vorbereiten des Entfernens einer Komponente mithilfe der Webbenutzeroberfläche 112
- Wiederinbetriebnehmen einer Komponente mithilfe der Webbenutzeroberfläche 113

Aktivieren und Deaktivieren von Komponenten 114

- Aktivieren und Deaktivieren von Komponenten mithilfe der CLI 114
- Aktivieren und Deaktivieren von Komponenten mithilfe der Webbenutzeroberfläche 114

Konfigurieren von Richtlinieneinstellungen 115

- Konfigurieren von Richtlinieneinstellungen mithilfe der CLI 115
- Konfigurieren von Richtlinieneinstellungen mithilfe der Webbenutzeroberfläche 116

**7. Systemüberwachung und Alarmverwaltung 117**

Informationen zur Systemüberwachung 118

Sensormesswerte 119

Ermitteln von Sensormesswerten mithilfe der Webbenutzeroberfläche 120

Ermitteln von Sensormesswerten mithilfe der CLI 121

System-LEDs 123

Unterstützte Zustände von System-LEDs 123

Anzeigen und Verwalten von LEDs mithilfe der Webbenutzeroberfläche 124

Anzeigen und Verwalten von LEDs mithilfe der CLI 125

ILOM-Ereignisprotokoll 126

Ereignisprotokoll-Zeitstempel und ILOM-Zeiteinstellungen 127

Unterstützte Zeiteinstellungen 127

Anzeigen und Festlegen von Zeiteinstellungen mithilfe der Webbenutzeroberfläche 127

Anzeigen und Festlegen von Zeiteinstellungen mithilfe der CLI 128

Syslog-Informationen 128

Fehlerverwaltung 129

Anzeigen des Fehlerstatus mithilfe der Webbenutzeroberfläche 130

Anzeigen des Fehlerstatus mithilfe der CLI 131

Überwachen von Systemsensoren, LEDs und des ILOM-Ereignisprotokolls 132

- Ermitteln des Zustands von LEDs mithilfe der Webbenutzeroberfläche 132
- Ermitteln von Sensormesswerten mithilfe der Webbenutzeroberfläche 133
- Anzeigen und Löschen des ILOM-Ereignisprotokolls mithilfe der Webbenutzeroberfläche 134
- Anzeigen und Löschen des ILOM-Ereignisprotokolls mithilfe der CLI 136

- Anzeigen und Konfigurieren von Zeiteinstellungen mithilfe der Webbenutzeroberfläche 138
- Konfigurieren von IP-Adressen von entfernten Syslog-Empfängern mithilfe der Webbenutzeroberfläche 139
- Konfigurieren von IP-Adressen von entfernten Syslog-Empfängern mithilfe der CLI 140

Informationen zur Alarmverwaltung 141

Konfiguration von Alarmregeln 141

Definitionen von Alarmregeleigenschaften 142

Verwalten von Alarmregelkonfigurationen mithilfe der ILOM-Webbenutzeroberfläche 145

Voraussetzungen 146

- Ändern von Alarmregelkonfigurationen mithilfe der Webbenutzeroberfläche 146
- Deaktivieren von Alarmregelkonfigurationen mithilfe der Webbenutzeroberfläche 147
- Erzeugen von Alarmtests mithilfe der Webbenutzeroberfläche 148

Verwalten von Alarmregelkonfigurationen mithilfe der ILOM-CLI 149

CLI-Befehle zum Verwalten von Alarmregelkonfigurationen 150

Voraussetzungen 152

- Ändern von Alarmregelkonfigurationen mithilfe der CLI 152
- Deaktivieren von Alarmregelkonfigurationen mithilfe der CLI 153
- Erzeugen von Alarmtests mithilfe der CLI 154

Konfigurieren eines SMTP-Clients für E-Mail-Benachrichtigungsalarme 155

- Aktivieren eines SMTP-Clients mithilfe der Webbenutzeroberfläche 156
- Aktivieren eines SMTP-Clients mithilfe der CLI 156

**8. Konfigurieren von ILOM-Kommunikationseinstellungen 159**

Verwalten von ILOM-Netzwerkeinstellungen mithilfe der CLI 160

Informationen zu Netzwerkeinstellungen 160

- Anzeigen von Netzwerkeinstellungen mithilfe der CLI 161
- Konfigurieren von Netzwerkeinstellungen mithilfe der CLI 161

Ziele, Eigenschaften und Werte 161

Serielle Anschlusseinstellungen 162

- Anzeigen von seriellen Anschlusseinstellungen mithilfe der CLI 163
- Konfigurieren von seriellen Anschlusseinstellungen mithilfe der CLI 163

Ziele, Eigenschaften und Werte 164

- Aktivieren von HTTP- oder HTTPS-Webzugriff mithilfe der CLI 164

Ziele, Eigenschaften und Werte 165

Konfigurieren von SSH-Einstellungen (Secure Shell) 166

- Herstellen einer sicheren entfernten Verbindung zum Ausführen von CLI-Befehlen 166
- Anzeigen des aktuellen Schlüssels mithilfe der CLI 166
- Aktivieren und Deaktivieren der SSH mithilfe der CLI 168
- Aktivieren und Deaktivieren der SSH mithilfe der Webbenutzeroberfläche 168
- Erzeugen eines neuen Schlüssels mithilfe der CLI 169
- Erzeugen eines neuen Schlüssels mithilfe der Webbenutzeroberfläche 169
- Neustart des SSH-Servers mithilfe der CLI 169
- Neustart des SSH-Servers mithilfe der Webbenutzeroberfläche 170

Verwalten von ILOM-Netzwerkeinstellungen mithilfe der Webbenutzeroberfläche 170

- Anzeigen von Netzwerkeinstellungen mithilfe der Webbenutzeroberfläche 170
- Konfigurieren von Netzwerkeinstellungen mithilfe der Webbenutzeroberfläche 171

- Anzeigen von seriellen Anschlusseinstellungen mithilfe der Webbenutzeroberfläche 172
- Konfigurieren von seriellen Anschlusseinstellungen mithilfe der Webbenutzeroberfläche 173
- Aktivieren von HTTP- oder HTTPS-Webzugriff mithilfe der Webbenutzeroberfläche 174

**9. Intelligent Platform Management Interface (IPMI) 177**

IPMI – Überblick 177

ILOM und IPMI 178

Verwenden von IPMItool 178

IPMI-Alarme 179

IPMItool-Beispiele 180

- Anzeigen einer Liste von Sensoren mit ihren Werten 180
- Anzeigen von Detailinformationen zu einem einzelnen Sensor 181
- Einschalten des Systems 181
- Ausschalten des Systems 181
- Aus- und Wiedereinschalten des Systems (Power Cycle) 181
- Ordnungsgemäßes Herunterfahren des Hosts 181
- Anzeigen von Herstellerinformationen für FRUs 182
- Anzeigen des IPMI-Systemereignisprotokolls (SEL) 183

**10. SNMP (Simple Network Management Protocol) 185**

SNMP – Überblick 186

Funktionsweise von SNMP 187

Grundlegende Dateien mit SNMP-Verwaltungsinformationen 188

Alarme und SNMP-Traps 189

Verwalten von SNMP mithilfe der CLI 189

- Hinzufügen eines SNMP-Benutzerkontos mithilfe der CLI 190
- Bearbeiten eines SNMP-Benutzerkontos mithilfe der CLI 190

- Löschen eines SNMP-Benutzerkontos mithilfe der CLI 190
- Hinzufügen oder Bearbeiten einer SNMP-Community mithilfe der CLI 190
- Löschen einer SNMP-Community mithilfe der CLI 191

Ziele, Eigenschaften und Werte 191

- Konfigurieren von SNMP-Trap-Zielen mithilfe der CLI 192

Verwalten von SNMP-Benutzern mithilfe der Webbenutzeroberfläche 193

- Konfigurieren von SNMP-Einstellungen mithilfe der Webbenutzeroberfläche 193
- Hinzufügen oder Bearbeiten eines SNMP-Benutzerkontos mithilfe der Webbenutzeroberfläche 194
- Löschen eines SNMP-Benutzerkontos mithilfe der Webbenutzeroberfläche 196
- Hinzufügen oder Bearbeiten einer SNMP-Community mithilfe der Webbenutzeroberfläche 196
- Löschen einer SNMP-Community mithilfe der Webbenutzeroberfläche 197
- Konfigurieren von SNMP-Trap-Zielen mithilfe der Webbenutzeroberfläche 198

SNMP-Beispiele 198

- Anzeigen und Konfigurieren von SNMP-Einstellungen 199
- Abrufen von Informationen mithilfe der Befehl `snmpget` oder `snmpwalk net-snmp` 200
- Festlegen von Informationen mithilfe von `snmpset` 201
- Empfangen von Traps mithilfe von `snmptrapd` 201

**11. Aktualisieren der ILOM-Firmware 203**

Prozess der Firmwareaktualisierung 203

ILOM-Firmwareaktualisierung – Überblick 204

- Anzeigen von ILOM-Versionsinformationen mithilfe der CLI 204
- Aktualisieren der ILOM-Firmware mithilfe der CLI 205

- Anzeigen von ILOM-Versionsinformationen mithilfe der Webbenutzeroberfläche 205
- Aktualisieren der ILOM-Firmware mithilfe der Webbenutzeroberfläche 206
- Zurücksetzen des ILOM-SP 207

**12. Entfernte Verwaltung von x64-Servern mithilfe der ILOM-Remotekonsole 209**

ILOM-Remotekonsole – Überblick 210

Einzel- und Mehrfachverwaltungsansichten für entfernte Hostserver 211

Voraussetzungen für die Installation 213

Anschlüsse und Protokolle für die Netzwerkkommunikation 213

Benutzerkonto mit Administrator-Rolle – Anmeldeauthentifizierung erforderlich 213

Starten und Konfigurieren von ILOM für die entfernte Verwaltung 214

- Herstellen einer Verbindung mit der ILOM-Webbenutzeroberfläche 215
- Konfigurieren von ILOM-Einstellungen für entfernte Steuerung mithilfe der Webbenutzeroberfläche 216

Starten und Konfigurieren der ILOM-Remotekonsole für die entfernte Verwaltung von x64-Servern 220

- Starten der ILOM-Remotekonsole mithilfe der ILOM-Webbenutzeroberfläche 220
- Hinzufügen einer neuen Serversitzung 222
- Starten, Beenden und Neustarten der Geräteumleitung 222
- Umleiten von Tastatur- und Mausgeräten 223
- Steuern von Tastaturmodi und Sendeoptionen für Tasten 224
- Umleiten von Speichergeräten 225
- Beenden der ILOM-Remotekonsole 226

Betriebsszenarien für die CD- und Diskettenumleitung 227

**A. Referenz für die ILOM-Befehlszeilenschnittstelle (CLI) 229**

Kurzreferenz für CLI-Befehle 229

Referenz für CLI-Befehle 235

**B. Glossar 251**

**Index 271**

# Vorwort

Im *Handbuch für den Integrated Lights Out Manager 2.0* werden die ILOM-Funktionen und -Aufgaben beschrieben, die für alle ILOM-unterstützenden Plattformen gelten. Sie erhalten in gleicher Weise Zugang zu den Funktionen und führen diese Aufgaben in gleicher Weise durch, unabhängig von der vom ILOM verwalteten Serverplattform. Weitere Benutzerdokumente beinhalten die ILOM-Funktionen und -Aufgaben, die für die von Ihnen verwendete Serverplattform spezifisch sind. Sie finden die ILOM-plattformspezifischen Informationen innerhalb des Dokumentationssatzes, der mit Ihrem System geliefert wurde.

**Hinweis –** Die Beschreibung in diesem Dokument ist auf die Server begrenzt, die ILOM unterstützen. In der Beschreibung bedeutet „alle Serverplattformen“ alle Fujitsu-Server, die ILOM unterstützen.
In Abhängigkeit von dem verwendeten Server werden einige der ILOM-Funktionen nicht unterstützt. Informieren Sie sich daher bitte vorher im ILOM-Ergänzungshandbuch und in den Produkthinweisen jedes Servers.

## Bevor Sie dieses Dokument lesen

Dieses Benutzerhandbuch enthält detaillierte Informationen über die ILOM-Merkmale und -Funktionen, die für alle vom ILOM verwalteten Serverplattformen gelten. Damit Sie alle in diesem Benutzerhandbuch enthaltenen Informationen verstehen und die Aufgaben ausführen können, sollten Sie dieses Dokument zusammen mit der ILOM-Dokumentation verwenden, die zum Lieferumfang Ihrer spezifischen Serverplattform gehört.

# ZUR GEWÄHRLEISTUNG EINES SICHEREN BETRIEBS

Dieses Handbuch enthält wichtige Informationen über den Gebrauch und die Handhabung des Produkts. Lesen Sie dieses Handbuch aufmerksam durch. Verwenden Sie das Produkt den in diesem Handbuch enthaltenen Anweisungen und Informationen entsprechend. Halten Sie dieses Handbuch stets zum weiteren Nachschlagen griffbereit.
Fujitsu gibt sich jede erdenkliche Mühe, um Benutzer und sich in deren Nähe befindliche Personen vor Verletzungen und Schäden an ihrem Eigentum zu bewahren. Verwenden Sie das Produkt nach Maßgabe dieses Handbuchs!

# Aufbau und Inhalt dieses Handbuchs

Dieses Handbuch ist wie folgt gegliedert:

- Kapitel 1 Introduction to ILOM

  Bietet einen Überblick über die ILOM-Merkmale und -Funktionen.

- Kapitel 2 Establish Initial Communication With ILOM

  Erläutert, wie Sie die anfängliche Kommunikation mit ILOM einrichten und welchen Aufgabentyp Sie mit verschiedenen Verbindungen durchführen können.

- Kapitel 3 ILOM Command-Line Interface and Log In

  Beschreibt, wie Sie die ILOM-CLI (Schnittstelle der ILOM-Befehlszeile) verwenden und wie Sie sich mit der CLI bei ILOM anmelden.

- Kapitel 4 ILOM Web Interface and Log In

  Beschreibt, wie Sie die ILOM-Webschnittstelle verwenden und wie Sie sich mit der Webschnittstelle bei ILOM anmelden.

- Kapitel 5 Manage User Accounts

  Erläutert, wie Sie Benutzerkonten mit ILOM-CLI oder der Webschnittstelle verwalten, sowie, wie Sie Active Directory, LDAP und RADIUS konfigurieren.

- Kapitel 6 Inventory and Component Management

  Beschreibt, wie Sie Komponenteninformationen anzeigen und ändern, wie Sie den Ausbau von Komponenten vorbereiten und Komponenten zur Wartung zurücksenden, und wie Sie die Richtlinieneinstellungen konfigurieren.

- Kapitel 7 System Monitoring and Alert Management

  Erläutert, wie Sie das System mit den Sensoren, Anzeigen und Ereignisprotokollen überwachen und wie Sie Alarme verwalten.

- Kapitel 8 Configure ILOM Communication Settings

  Bietet eine Übersicht über die ILOM-Netzwerkeinstellungen und die Aufgaben, die Sie durchführen müssen, um die Netzwerkeinstellungen mit ILOM-CLI oder der Webschnittstelle zu konfigurieren.

- Kapitel 9 Intelligent Platform Management Interface

  Beschreibt das Intelligent Platform Management Interface (IPMI) und IPMItool.

- Kapitel 10 Simple Network Management Protocol

  Erläutert, wie SNMP arbeitet, und wie Sie SNMP-Benutzer mit ILOM-CLI oder der Webschnittstelle verwalten.

- Kapitel 11 Update ILOM Firmware

  Erläutert, wie Sie die ILOM-Firmware mit ILOM-CLI oder der Webschnittstelle upgraden und zurücksetzen.

- Kapitel 12 Remote Management of x64 Servers Using the ILOM Remote Console

  Beschreibt die ILOM-Fernbedienungsanwendung und wie Sie die Fernbedienung starten und konfigurieren, um eine Serverplattform aus der Ferne zu verwalten.

- Anhang A ILOM Command-Line Interface Reference

  Bietet eine Referenz zu Befehlen der ILOM-CLI und erläutert, wie Sie die Befehle verwenden.

- Anhang B Glossary

  Bietet die Definitionen einiger Wörter und Phrasen, die in diesem Benutzerhandbuch verwendet werden.

- Index

  Enthält Stichwörter und die entsprechenden Referenzseitennummern, um erforderlichenfalls auf einfache Art und Weise bestimmte Themen in diesem Handbuch auffinden zu können.

# Dokumentationen

Die neuesten Versionen aller Handbücher für die SPARC-Enterprise-Serie sind auf den folgenden Websites verfügbar:

Globale Site

`http://www.fujitsu.com/sparcenterprise/manual/`

Japanische Site

`http://primeserver.fujitsu.com/sparcenterprise/manual/`

| Titel | Beschreibung | Handbuch-Code |
|---|---|---|
| *Integrated Lights Out Manager 2.0 – Erganzungshandbuch fur SPARC Enterprise T5120 und T5220 Server* | Zur Verwendung der Software „Integrated Lights Out Manager (ILOM)“ auf den Servern | C120-E465 |

# Verwendung von UNIX-Befehlen

Dieses Dokument enthält möglicherweise keine Informationen über grundlegende UNIX®-Befehle und -Vorgehensweisen wie das Herunterfahren und Hochfahren des Systems und die Gerätekonfiguration. Informieren Sie sich darüber bitte anhand der folgenden Dokumentationen:

- anhand der Software-Dokumentation, die Sie zusammen mit Ihrem System erhalten haben
- anhand der Solaris™ Betriebssystem-Dokumentation unter:

  `http://docs.sun.com`

# Textkonventionen

In diesem Handbuch werden die folgenden Symbole zur Kennzeichnung bestimmter Informationsarten verwendet.

| Schrifttyp* | Bedeutung | Beispiel |
|---|---|---|
| `AaBbCc123` | Befehl-, Datei- und Verzeichnisnamen; Computerbildschirmausgabe | Editieren Sie Ihre `.login` file.<br>Benutzen Sie `ls -a` um alle Datei zu verzeichnen.<br>`% You have mail.` |
| **`AaBbCc123`** | Ihre Eingabe im Fall der Kontrastierung mit der Computerbildschirmausgabe | `% su`<br>`Password:` |
| *AaBbCc123* | Buchtitel, neue Wörter oder Ausdrücke und zu betonende Wörter.<br>Ersetzung von Befehlszeilenvariablen durch Echtnamen oder -werte. | Lesen Sie Kapitel 6 in der *Benutzeranleitung*.<br>Diese werden als *class*-Optionen bezeichnet.<br>Um dies tun zu können, *müssen* Sie Überbenutzer sein.<br>Geben Sie rm *filename* ein. |

* Die Einstellungen Ihres Browsers unterscheiden sich möglicherweise von diesen Einstellungen.

# Fujitsu begrüßt Ihre Kommentare

Wir würden uns über Ihre Kommentare zu diesem Dokument und Ihre Verbesserungsvorschläge freuen.
Sie können uns diese mittels des „Leserkommentarformulars“ zukommen lassen.

# Formular für Leserkommentare

We would appreciate your comments and suggestions for improving this publication.

Date:_____ Publication No.:
Your Name:_____ Publication Name:
Company: _____
Address: _____
City/State/Zip:_____
Phone/Email address: _____

Your Comments:

| Page | Line | Comments |
|---|---|---|
| | | |
| Reply requested: o Yes o No | | |

Please evaluate the overall quality of this manual by checking ( ✓ )the appropriate boxes

| | Good | Fair | Poor | | Good | Fair | Poor | | Good | Fair | Poor |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Organization: | o | o | o | Use of examples: | o | o | o | Legibility: | o | o | o |
| Accuracy: | o | o | o | Index coverage: | o | o | o | Binding: | o | o | o |
| Clarity: | o | o | o | Cross | | | | Figures and tables: | o | o | o |
| Overall rating of | | | | referencing: | o | o | o | General appearance: | o | o | o |
| this publication: | o | o | o | | | | | | | | |

Technical level: o Too detailed o Appropriate o Not enough detail

All comments and suggestions become the property of Fujitsu Limited.

**For Users in U.S.A., Canada, and Mexico**

Fold and fasten as shown on back
No postage necessary if mailed in U.S.A.

Fujitsu Computer Systems
Attention: Engineering Ops M/S 249
1250 East Arques Avenue
P.O. Box 3470
Sunnyvale, CA 94088-3470
FAX: (408) 746-6813

**For Users in Other Countries**

Fax this form to the number below or send this form to the address below.

Fujitsu Learning Media Limited
FAX: 81-3-3730-3702
37-10 Nishi-Kamata 7-chome
Oota-Ku
Tokyo 144-0051
JAPAN

FUJITSU LIMITED

FOLD AND TAPE

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

# BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO 741 SUNNYVALE CA

POSTAGE WILL BE PAID BY ADDRESSEE

FUJITSU

FUJITSU COMPUTER SYSTEMS
AT TENTION ENGINEERING OPS M/S 249
1250 EAST ARQUES AVENUE
P O BOX 3470
SUNNYVALE CA 94088-3470

FOLD AND TAPE

KAPITEL 1

# Einführung in ILOM

Integrated Lights Out Manager (ILOM) 2.0 ist die Systemverwaltungs-Firmware, mit der Sie eine Vielzahl unterschiedlicher Serverplattformen überwachen, verwalten und konfigurieren können.

Dieses Kapitel enthält folgende Abschnitte:


- „Was ist ILOM?“ auf Seite 1
- „ILOM auf SP und CMM“ auf Seite 2
- „ILOM-Schnittstellen“ auf Seite 3
- „ILOM-Verwaltungsnetzwerk“ auf Seite 4
- „ILOM-Verbindungsmethoden“ auf Seite 5
- „Rollen für ILOM-Benutzerkonten“ auf Seite 6
- „Vorkonfiguriertes ILOM-Administratorkonto“ auf Seite 6
- „ILOM-Leistungsmerkmale“ auf Seite 7
- „Neue Leistungsmerkmale in ILOM 2.0“ auf Seite 9


## Was ist ILOM?

Integrated Lights Out Manager (ILOM) ist eine Systemverwaltungs-Firmware, die auf einigen Serverplattformen vorinstalliert ist. ILOM ermöglicht die aktive Verwaltung und Überwachung der in Ihren Serversystemen installierten Komponenten. Mit ILOM können Sie Ihr System proaktiv überwachen und verwalten, indem Sie unter anderem Hardwarekonfigurationen anzeigen, Systeminformationen überwachen und Systemalarme verwalten. ILOM bietet eine browserbasierte Webbenutzeroberfläche und eine Befehlszeilenschnittstelle (Command-Line Interface, CLI) sowie eine SNMP- und eine IPMI-Schnittstelle.

ILOM wird automatisch initialisiert, sobald das System mit Strom versorgt wird. ILOM wird unabhängig vom Zustand des Hostbetriebssystems ausgeführt, was es zu einem „Lights-Out"-Verwaltungssystem macht.

Zu den wesentlichen Leistungsmerkmalen von ILOM gehören unter anderem:

- Ausführung mit eigenem Prozessor und eigenen Ressourcen.
- Ermöglicht die Verwaltung des Servers ohne Belastung von Systemressourcen.
- Bereitstellung der Verwaltungsfunktionen durch Ausnutzung der Standby-Stromversorgung auch bei ausgeschaltetem Server.
- Bereitstellung eines vom Datennetzwerk getrennten, isolierten Verwaltungsnetzwerks.
- Bereitstellung einer exakten Übersicht von Hardwarebestand und -umgebung.
- Bereitstellung von Funktionen für Stromversorgungssteuerung, Komponentenverwaltung und Hostkonsolenzugriff.
- Funktion als Integrationspunkt für weitere Verwaltungstools, wie z. B. SUN N1™ System Manager und Anwendungen von Fremdherstellern.
- Möglichkeit zum Herunterladen von SP-Firmware (Service-Prozessor)- und BIOS-Änderungen.
- Verwaltung des Bestands von Hot-Plug-Systemkomponenten.

# ILOM auf SP und CMM

ILOM wird auf einer Reihe verschiedener Serverplattformen, einschließlich Rack-System-Servern und Blade-Servern, unterstützt. Die ILOM-Firmware ist auf dem Service-Prozessor (SP) von Rack-System-Servern und Blade-Servern vorinstalliert, bzw. auf dem Chassis Monitoring Module (CMM), falls dies auf Ihre Serverplattform zutrifft.

ILOM unterstützt zwei Methoden der Systemverwaltung: direkte Verwendung des SP oder gegebenenfalls Verwendung des CMM.

- **Direkte Verwendung des Service-Prozessors** – Die Verwaltung der SPs von Rack-System-Servern durch direkte Kommunikation mit dem SP oder dem Blade ermöglicht die Verwaltung einzelner System- bzw. Blade-Vorgänge. Diese Vorgehensweise kann bei der Behebung von Fehlern eines Service-Prozessors oder der Steuerung des Zugriffs auf bestimmte Systeme oder Blades hilfreich sein, wenn ein Mehrbenutzersystem vorliegt.
- **Verwenden des CMM (Chassis Monitoring Module)** – Wenn Ihr System mit einem CMM ausgerüstet ist und Sie das System über das CMM verwalten, können Sie Komponenten innerhalb des gesamten Systems einrichten und verwalten oder auf die Detailebene wechseln, um einzelne Blade-Server-SPs zu verwalten.

# ILOM-Schnittstellen

Auf ILOM kann über eine Reihe verschiedener Schnittstellen bzw. Benutzeroberflächen zugegriffen werden.

- **Webbenutzeroberfläche** – Die Webbenutzeroberfläche bietet eine einfach zu bedienende Browseroberfläche, die das Anmelden beim SP und das Durchführen von Systemverwaltungs-, -überwachungs- und IPMI-Aufgaben ermöglicht. Informationen zur ILOM-Webbenutzeroberfläche finden Sie in Kapitel 4.
- **Befehlszeilenschnittstelle (Command-Line Interface, CLI)** – Die CLI ermöglicht den Betrieb von ILOM mithilfe von Tastaturbefehlen, wobei sie sich an CLIs und Skriptprotokollen gemäß Industriestandard orientiert: DMTF „SMASH“ CLP. Sie können ein Terminal oder einen Computer, auf dem Terminalemulationssoftware ausgeführt wird, direkt am seriellen Systemanschluss anschließen oder mithilfe einer SSH (Secure Shell) eine Verbindung am Ethernet-Netzwerkverwaltungsanschluss herstellen. Informationen zur CLI finden Sie in Kapitel 3.
- **Remotekonsole** – Die ILOM-Remotekonsole ermöglicht den entfernten Zugriff auf die Konsole des Servers. Hierbei werden Tastatur, Maus und Bildschirmanzeige umgeleitet. Außerdem können Ein- und Ausgaben von CD-ROM- und Diskettenlaufwerken, die sich am lokalen Computer befinden, umgeleitet werden. Informationen zur Remotekonsole finden Sie in Kapitel 12.
- **Intelligent Platform Management Interface (IPMI)** – Mithilfe von IPMI v1.5 und v2.0 sowie dem Dienstprogramm „IPMItool“ können Sie Geräte verwalten und konfigurieren und unter Verwendung einer CLI Informationen vom BMC (Baseboard Management Controller) des Systems abzurufen. Mit IPMItool können Sie den Status von Hardwarekomponenten entfernt überwachen, Systemprotokolle überwachen, Berichte über austauschbare Komponenten empfangen und die Serverkonsole umleiten. Weitere Informationen zu IPMI finden Sie in Kapitel 9.
- **SNMP-Schnittstelle (Simple Network Management Protocol)** – ILOM bietet ebenfalls eine SNMP v3.0-Schnittstelle (mit eingeschränkter Unterstützung von SNMP v1 und SNMP v2c) für externe Rechenzentren-Verwaltungsanwendungen wie Sun N1™ System Manager oder Anwendungen von Fremdherstellern wie Hewlett-Packard OpenView® oder IBM Tivoli®. Weitere Informationen zu SNMP finden Sie in Kapitel 10.

# ILOM-Verwaltungsnetzwerk

Ihre Serverplattform ist mit einem Netzwerkverwaltungsanschluss sowie einem Datenanschluss ausgestattet. Diese getrennten physikalischen Ethernet-Anschlüsse stehen für ILOM und die auf der Hosthardware ausgeführten Betriebssysteme zur Verfügung. Sie können Ihre Serverplattform mit ILOM verwalten, indem Sie eine Verbindung mit dem dedizierten Netzwerkverwaltungsanschluss herstellen. Wenn Sie eine Verbindung mit ILOM über den Netzwerkverwaltungsanschluss herstellen, wird der an ILOM gerichtete Verwaltungsdatenverkehr von allen anderen Datenübertragungen des Betriebssystemhosts getrennt. Über den Netzwerkanschluss wird kein Datenverkehr übermittelt. Dies ermöglicht im Bedarfsfall die vollständige Isolierung des Verwaltungsverkehrs in einem gesonderten Netzwerk.

Die Position und Beschriftung des Netzwerkverwaltungsanschlusses ist bei jedem System individuell unterschiedlich. Zusätzlich beeinflusst der Typ der Serverplattform, wie die interne Verwaltungskommunikation bereitgestellt wird. Auf einem Blade-Serversystem stellt der Netzwerkanschluss beispielsweise eine Verbindung mit allen CMMs und SPs im Gehäuse bereit. Informationen darüber, wie Ihr System die interne Verwaltungskommunikation bereitstellt, finden Sie in der dazugehörigen Plattformdokumentation.

Wenn Sie nicht ILOM und den Netzwerkverwaltungsanschluss zum Verwalten des Servers einsetzen, sind zahlreiche der erweiterten Leistungsmerkmale wie Umgebungsüberwachung, IPMI-Verwaltung und die Webbenutzeroberfläche nicht verfügbar. Mithilfe des Datenanschlusses des Hostbetriebssystems können Sie zwar auf Netzwerkverwaltungsanwendungen von Fremdherstellern, SNMP-Tools und Betriebssystem-Dienstprogramme zugreifen, doch diese Lösungen verfügen nur über einen eingeschränkten Zugriff auf die Plattform. Eine weitere Möglichkeit zur lokalen Verwaltung des Servers besteht darin, mithilfe eines Computers, auf dem Terminalemulationssoftware ausgeführt wird, oder eines Terminals eine Verbindung über den seriellen Anschluss des Servers herzustellen. Beachten Sie, dass ohne jegliche direkte Verbindung mit ILOM keine entfernte Verwaltung der Serverplattform möglich ist.

# ILOM-Verbindungsmethoden

Die zum Herstellen einer Verbindung mit ILOM verwendete Methode hängt von der Serverplattform ab.

In der folgenden Tabelle werden die verschiedenen Methoden aufgeführt, mit deren Hilfe eine Verbindung mit ILOM hergestellt werden kann.

**TABELLE 1-1** ILOM-Verbindungsmethoden

| Verbindungs-methode | Rack-System | Blade | Unterstützte Schnittstelle/ Benutzeroberfläche | Beschreibung |
|---|---|---|---|---|
| Ethernet-Netz-werkverwal-tungsverbindung | Ja | Ja | CLI und Webbenut-zeroberfläche | Herstellen einer Verbindung am Ethernet-Netzwerkverwaltungsanschluss. Hierzu müssen Sie die IP-Adresse von ILOM kennen. Diese Methode unterstützt die Webbenutzeroberfläche und die CLI. |
| Serielle Verbindung über Server oder Blade | Ja | Nein | Nur CLI | Direktes Anschließen am seriellen Verwaltungsanschluss des Servers oder Blades. Verwenden Sie nötigenfalls ein serielles Adapterkabel für den Anschluss am seriellen Anschluss. Diese Methode unterstützt nur die CLI. |
| Serielle Verbindung über CMM | Nein | Ja | Nur CLI | Anschließen am seriellen Anschluss des CMM. Diese Methode unterstützt nur die CLI. |

**Hinweis –** ILOM unterstützt maximal 10 aktive Sitzungen, einschließlich serieller, SSH (Secure Shell)- und Webbenutzeroberflächensitzungen.

Um mithilfe der ILOM-Webbenutzeroberfläche oder -CLI auf das Verwaltungsnetzwerk zuzugreifen, benötigen Sie die IP-Adresse des zu verwaltenden CMM oder SP. Jedem CMM und SP wird während der ersten Systemeinrichtung eine eindeutige IP-Adresse zugewiesen. Informationen zum Zuweisen anfänglicher IP-Adressen für SPs und CMMs finden Sie in Kapitel 2.

# Rollen für ILOM-Benutzerkonten

ILOM-Benutzerkonten verfügen über definierte Rollen, die ILOM-Benutzerzugriff und -rechte festlegen. Administratoren können Benutzerkonten mithilfe der ILOM-Webbenutzeroberfläche oder -CLI verwalten.
Folgende Rollen sind ILOM-Konten zugewiesen:

- **Administrator** – Ermöglicht den Zugriff auf alle ILOM-Leistungsmerkmale, -Funktionen und -Befehle.
- **Operator** – Ermöglicht die Verwaltung und Überwachung des Hostsystems in vollem Umfang und bietet schreibgeschützten Zugriff auf die ILOM-Konfiguration.

# Vorkonfiguriertes ILOM-Administratorkonto

In ILOM ist ein vorkonfiguriertes Administratorkonto vorinstalliert:

- Benutzername: `root`
- Passwort: `changeme`

Das vorkonfigurierte Administratorkonto, auch bekannt als „root“, kann weder gelöscht noch geändert werden. Das Standardpasswort (`changeme`) kann dagegen geändert werden. Dieses Konto bietet integrierte Administratorberechtigungen (Lese- und Schreibzugriff) für alle ILOM-Leistungsmerkmale, -Funktionen und -Befehle.

Beim ersten Zugriff auf ILOM auf SP- oder CMM-Ebene müssen Sie sich als „root“ mit dem Standardpasswort `changeme` anmelden. Nachdem Sie sich bei ILOM angemeldet und eine Netzwerkverbindung mit dem System hergestellt haben, müssen Sie das Standardpasswort (`changeme`), das dem root-Konto von ILOM zugeordnet ist, ändern. Ändern Sie das Passwort auf jedem in Ihrem System installierten SP und CMM, um das System vor nicht autorisierten Zugriffen zu schützen. Informationen zum Ändern des Passworts des root-Kontos von ILOM finden Sie unter „Zurücksetzen des ILOM-SP“ auf Seite 207.

# ILOM-Leistungsmerkmale

In Tabelle 1-1 werden die ILOM-Leistungsmerkmale und -Aufgaben aufgeführt, die auf allen Systemen verfügbar sind, die ILOM unterstützen. Informationen darüber, ob das jeweilige Leistungsmerkmal auf Ihrem System unterstützt wird, finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

**TABELLE 1-2** ILOM-Leistungsmerkmale

| Leistungsmerkmal | Kundenvorteil |
|---|---|
| SCHNITTSTELLEN | |
| Webbenutzeroberfläche | • Bereitstellung einer browserbasierten Benutzeroberfläche. |
| Befehlszeilenschnittstelle (CLI) | • Unterstützung von CLIs und Skriptprotokollen gemäß Industriestandard: DMTF „SMASH“ CLP.<br>• Wiederverwendbarkeit von auf Systemen vorhandenen Skripts, Automatisierung von Aufgaben mithilfe vertrauter Schnittstellen. |
| Systemverwaltungsschnittstellen | • Unterstützung von SNMP v1, v2c, v3 und IPMI v1.5 und v2.0 gemäß Industriestandard. Bereitstellung der Plattformverwaltung mithilfe von SNMP durch die Plattform-MIB zusätzlich zu IPMI. Mögliche Integration von benutzerdefinierten oder Fremdhersteller-Verwaltungsanwendungen in ILOM mithilfe der Steuerungs-MIB.<br>• Bereitstellung des Zugriffs auf entfernte Systeme mithilfe der ILOM-Remotekonsole. |
| SICHERHEIT | |
| SSH 2.0-Unterstützung | • Möglichkeit sicheren Zugriffs auf die CLI. |
| LDAP, MSFT Active Directory, RADIUS | • Unterstützung von Authentifizierungs- und Autorisierungsprotokollen gemäß Industriestandard zur leichteren Integration in vorhandene Umgebungen. |
| Benutzerverwaltung | • Unterstützung von Administrator- und Operator-Rollen mit konfigurierbaren Zugriffsstufen für erhöhte Sicherheit und Kontrolle des Systems. |
| Funktion zum Zurücksetzen des root-Passworts | • Verhinderung von nicht autorisiertem Zugriff auf das System. Zurücksetzen des Passworts durch Drücken eines Schalters oder Stecken/Ziehen eines Jumpers. |
| SSL-Zertifikat | • Möglichkeit der sicheren Kommunikation mithilfe von SSL-Standardzertifikaten sowie selbstsignierten Schlüsseln für den HTTPS-Zugriff. |

**TABELLE 1-2** ILOM-Leistungsmerkmale *(Fortsetzung)*

| Leistungsmerkmal | Kundenvorteil |
|---|---|
| LOKALER UND ENTFERNTER ZUGRIFF | |
| Zugriff auf den SP bei ausgeschaltetem Host | • Möglichkeit des kontinuierlichen ILOM-Betriebs, unabhängig vom Zustand des Hostbetriebssystems. |
| Dedizierter Netzwerkverwaltungsanschluss | • Trennung des Netzwerkverwaltungsverkehrs vom Datennetzwerkverkehr. |
| Remotekonsole | • Bereitstellung einer einfachen Webbenutzeroberfläche für den Zugriff auf entfernte Systeme. Anmelden am SP zum Starten der Remotekonsole ist nicht mehr erforderlich. |
| Bearbeitbares Hostname-Datenfeld | • Möglichkeit für Administratoren, das Hostname-Datenfeld zusätzlich zur IP-Adresse für die Systemkennung zu verwenden. |
| De-/aktivierbare Webbenutzeroberfläche | • Einschränkung des ILOM-Zugriffs und Ermöglichung des reinen CLI-Zugriffs. |
| ÜBERWACHUNG UND PROTOKOLLIERUNG | |
| SNMP- und IPMI-Überwachung und -Steuerung | • Überwachung von Komponenten mithilfe von SNMP-Befehlen gemäß Industriestandard und dem IPMI-Dienstprogramm „IPMItool“. |
| Ereignisprotokollierung | • Bereitstellung einer konsistenten Methode zum Protokollieren aller Betriebsdaten. |
| Konfigurierbare Alarmschwellenwerte | • Möglichkeit für Benutzer, den SP so zu konfigurieren, dass bei Überschreiten eines Systemschwellenwerts ein IPMI PET-Alarm gesendet wird. |
| E-Mail-Ereignisbenachrichtigung | • Bereitstellung der schnellen und bequemen Benachrichtigung über Ereignisse. |
| Meldung von hardware- und systembezogenen Fehlern sowie ECC-Arbeitsspeicherfehlern in SP-Protokolle, Syslog und entfernten Protokollhost | • Möglichkeit der schnelleren Fehlerdiagnose und -eingrenzung und dadurch kürzere Ausfallzeiten. |
| STROMVERSORGUNGSSTEUERUNG | |
| Erzwungenes Ausschalten | • Möglichkeit von Notfallsystemabschaltungen. |
| Ordnungsgemäßes Herunterfahren und Ausschalten | • Möglichkeit für Benutzer, das Hostbetriebssystem vor dem Ausschalten des Systems herunterzufahren. |
| Entferntes Ein- und Ausschalten | • Möglichkeit für Benutzer, die Systemstromversorgung entfernt zu steuern. |
| FIRMWARE | |
| Identifizierung der Firmwareversionen über die Webbenutzeroberfläche oder CLI | • Bereitstellung einer einfachen Methode zum Identifizieren von Firmwareversionen. |
| Firmwareaktualisierungen über die Webbenutzeroberfläche oder CLI | • Bereitstellung einfacher Verfahren zum Aktualisieren der Firmware. |

**TABELLE 1-2** ILOM-Leistungsmerkmale *(Fortsetzung)*

| Leistungsmerkmal | Kundenvorteil |
|---|---|
| KONFIGURATION | |
| Manuelle SP-Konfiguration, einschließlich IP-Adresse, über die BIOS-Schnittstelle, serielle oder Ethernet-SP-Anschlüsse oder das Hostbetriebssystem | • Vereinfachung der Erstkonfiguration. |
| Über lokale Tastatur und Bildschirm programmierbare SP-IP-Adresse | • Vereinfachung der manuellen IP-Konfiguration für Systeme in Rechenzentren. |

# Neue Leistungsmerkmale in ILOM 2.0

- Active Directory
- E-Mail-Alarme
- Neue, aktualisierte MIBs
- SNMP-Traps
- Internationalisierung der Remotekonsole

KAPITEL 2

# Herstellen der ersten Kommunikation mit ILOM

Die Kommunikation mit ILOM kann über eine Konsolenverbindung mit dem seriellen Verwaltungsanschluss des Servers oder CMM bzw. über eine Ethernet-Verbindung am Netzwerkverwaltungsanschluss des Servers oder CMM hergestellt werden.

Der Typ der Verbindung, die mit ILOM hergestellt wird, bestimmt die Art der Aufgaben, die durchgeführt werden können. Für einen entfernten Zugriff auf den vollen Umfang der Systemverwaltungsfunktionen in ILOM sind beispielsweise sowohl eine Ethernet-Verbindung als auch eine IP-Zuweisung mit dem Server-SP sowie gegebenenfalls dem CMM erforderlich.

Dieses Kapitel enthält folgende Abschnitte:


- „Erste ILOM-Einrichtung“ auf Seite 12
  - „Arbeitsblatt für die erste Einrichtung“ auf Seite 12
  - „Aspekte bei der IP-Zuweisung über DHCP“ auf Seite 15
  - „Aspekte bei der Zuweisung statischer IPs“ auf Seite 18
  - „Konfiguration von Verwaltungsnetzwerk-IP-Adressen“ auf Seite 20
  - „Zuweisen von ILOM-Netzwerkanschlüssen“ auf Seite 20
  - „Hostnamenkennung für Server-SP und CMM“ auf Seite 22
  - „Systemkennungs-Textzeichenfolgen für Server“ auf Seite 22
- „Zuweisen von IP-Adressen zu den Serverplattform-SP-Schnittstellen“ auf Seite 23
  - „Zuweisen von IP-Adressen über DHCP mithilfe einer Ethernet-Verwaltungsverbindung“ auf Seite 23
  - „Zuweisen einer statischen IP-Adresse zum Server-SP mithilfe einer seriellen Verbindung“ auf Seite 25
  - „Zuweisen einer statischen IP-Adresse zum CMM mithilfe einer seriellen Verbindung“ auf Seite 27

- „Bearbeiten von IP-Adressenzuweisungen mithilfe einer Ethernet-Verwaltungsverbindung“ auf Seite 29
  - „Bearbeiten vorhandener IP-Adressen in ILOM mithilfe der Webbenutzeroberfläche“ auf Seite 29
  - „Bearbeiten vorhandener IP-Adressen in ILOM mithilfe der CLI“ auf Seite 31
- „Zuweisen von Hostnamen oder Systemkennungen“ auf Seite 33


# Erste ILOM-Einrichtung

Vor dem Herstellen der Kommunikation mit ILOM müssen Sie folgende Themen lesen:


- „Arbeitsblatt für die erste Einrichtung“ auf Seite 12
- „Aspekte bei der IP-Zuweisung über DHCP“ auf Seite 15
- „Aspekte bei der Zuweisung statischer IPs“ auf Seite 18
- „Konfiguration von Verwaltungsnetzwerk-IP-Adressen“ auf Seite 20
- „Zuweisen von ILOM-Netzwerkanschlüssen“ auf Seite 20
- „Hostnamenkennung für Server-SP und CMM“ auf Seite 22
- „Systemkennungs-Textzeichenfolgen für Server“ auf Seite 22


## Arbeitsblatt für die erste Einrichtung

Verwenden Sie das folgende Arbeitsblatt in TABELLE 2-1, um die Informationen zu sammeln, die zum Herstellen einer ersten Kommunikation mit ILOM erforderlich sind.

**TABELLE 2-1** Arbeitsblatt für die erste Einrichtung zum Herstellen der Kommunikation mit ILOM

| Informationen für die Einrichtung | Anforderung | Beschreibung |
|---|---|---|
| Lokale serielle Konsolenverbindung | Optional – *bei Verwendung von DHCP zum Zuweisen der anfänglichen IP-Adresse*<br><br>Obligatorisch – *bei Nichtverwendung eines DHCP-Servers zum Zuweisen der anfänglichen IP-Adresse* | Wenn Sie keinen DHCP-Server verwenden, um dem Server-SP oder CMM IP-Adressen zuzuweisen, müssen Sie eine lokale serielle Konsolenverbindung mit ILOM über den seriellen Verwaltungsanschluss des Servers oder CMM (Chassis Monitoring Module) herstellen.<br>Weitere Informationen zum Anschließen einer seriellen Konsole an einen Server oder ein CMM finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt. |
| Entfernte Ethernet-Verwaltungsverbindung | Optional | Schließen Sie ein Netzwerkkabel (Ethernet) am Netzwerkverwaltungsanschluss des Servers oder CMM an. Die am Netzwerkverwaltungsanschluss angebrachte Bezeichnung kann in Abhängigkeit von der Serverplattform unterschiedlich sein. Einige Server- und CMM-Netzwerkverwaltungsanschlüsse sind mit NET MGT oder MGT bezeichnet. Bei Fragen zur Bezeichnung des Netzwerkverwaltungsanschlusses bzw. zum Anschließen eines Ethernet-Kabels am Verwaltungsanschluss ziehen Sie die Benutzerdokumentation heran, die der jeweiligen Serverplattform beiliegt.<br>Um auf den gesamten Umfang der Verwaltungsfunktionen von ILOM zugreifen zu können, müssen Sie eine Verbindung zwischen dem lokalen Netzwerk (LAN) und dem Netzwerkverwaltungsanschluss eines Servers oder CMM herstellen.<br>Beachten Sie, dass alle eigenständigen Rack-System-Standalone-Server mit einem Netzwerkverwaltungsanschluss ausgestattet sind. Blade-Servermodule verfügen jedoch über keinen solchen Anschluss. Eine Ethernet-Verbindung mit Blade-Servermodulen wird über den Netzwerkverwaltungsanschluss am CMM hergestellt. |
| Zuweisung einer SP-IP | Obligatorisch | Entscheiden Sie, ob den Server-SPs oder CMMs IP-Adressen über DHCP oder statisch zugewiesen werden. Die gesamte entfernte Systemverwaltungskommunikation mit ILOM erfolgt über das Server-SP- oder CMM-Verwaltungsnetzwerk.<br>Weitere Informationen erhalten Sie in folgenden Themen:<br>• „Aspekte bei der IP-Zuweisung über DHCP“ auf Seite 15<br>• „Aspekte bei der Zuweisung statischer IPs“ auf Seite 18<br>• „Zuweisen von IP-Adressen zu den Serverplattform-SP-Schnittstellen“ auf Seite 23 |

**TABELLE 2-1** Arbeitsblatt für die erste Einrichtung zum Herstellen der Kommunikation mit ILOM *(Fortsetzung)*

| Informationen für die Einrichtung | Anforderung | Beschreibung |
|---|---|---|
| ILOM-Schnittstelle | Obligatorisch | Beim Zuweisen (oder Ändern) einer IP-Adresse zu einem Server-SP oder CMM wird eine der folgenden ILOM-Schnittstellen verwendet:<br>• **Befehlszeilenschnittstelle (Command-line interface, CLI) – zum Zuweisen der anfänglichen IP-Adresse**. Wenn dem Server-SP oder CMM keine IP-Adresse zugewiesen wurde, können Sie eine Verbindung mit ILOM herstellen, um die IP-Adresse über eine lokale serielle Konsole zuzuweisen.<br>Die CLI wird normalerweise für alle Aufgaben eingesetzt, die in ILOM über eine serielle Verbindung (lokale serielle Konsole, Terminalemulationsanwendung oder entfernte SSH-Verbindung) durchgeführt werden.<br>• **Webbenutzeroberfläche – zum Bearbeiten einer vorhandenen IP-Adresse**. Wenn dem Server-SP oder CMM eine IP-Adresse zugewiesen wurde und eine LAN-Verbindung mit dem MGT-Anschluss hergestellt ist, können Sie eine Verbindung mit ILOM herstellen, um die vorhandenen IP-Adressen über die Webbenutzeroberfläche zu bearbeiten.<br>Die Webbenutzeroberfläche wird normalerweise für alle Aufgaben verwendet, die in ILOM über eine Ethernet-Verwaltungsverbindung durchgeführt werden.<br>Weitere Informationen zu ILOM-Schnittstellen finden Sie in Kapitel 3 und Kapitel 4. |
| ILOM-Firewallzugriff | Optional | Informationen zu Ethernet-Netzwerken, die Firewallzugriff benötigen, finden Sie unter der Verwendung des Netzwerkanschlusses durch ILOM. Weitere Informationen zu diesem Thema finden Sie unter „Zuweisen von ILOM-Netzwerkanschlüssen“ auf Seite 20. |
| Zuweisung eines SP-Hostnamens | Optional | Einem Server-SP kann optional ein aussagekräftiger Hostname zugewiesen werden. Weitere Informationen hierzu finden Sie unter „Hostnamenkennung für Server-SP und CMM“ auf Seite 22 und „Zuweisen von Hostnamen oder Systemkennungen“ auf Seite 33. |
| Zuweisung einer Systemkennung | Optional | Einem Server kann optional eine Systemkennung (aussagekräftiger Name) zugewiesen werden. Weitere Informationen hierzu finden Sie unter „Hostnamenkennung für Server-SP und CMM“ auf Seite 22 und „Zuweisen von Hostnamen oder Systemkennungen“ auf Seite 33. |

# Aspekte bei der IP-Zuweisung über DHCP

Wen Sie beabsichtigen, einem Server-SP oder CMM eine IP-Adresse über einen DHCP-Server (Dynamic Host Configuration Protocol) zuzuweisen, finden Sie Informationen hierzu in folgenden Themen:


- „Senden des DHCPDISCOVER-Pakets auf Serverplattformen“ auf Seite 15
- „Voraussetzungen für die Zuweisung über DHCP“ auf Seite 15
- „MAC-Adresse der SP-Netzwerkschnittstelle“ auf Seite 16
- „Anforderungen nach der Zuweisung über DHCP“ auf Seite 17


## Senden des DHCPDISCOVER-Pakets auf Serverplattformen

Der Server-SP bzw. das CMM sendet automatisch ein DHCPDISCOVER-Paket, sobald die Stromversorgung der Serverplattform hergestellt ist. Wenn sich bereits ein eingerichteter DHCP-Server im Netzwerk befindet, gibt dieser automatisch ein DHCPOFFER-Paket mit IP-Adressen und weiteren Netzwerkkonfigurationsinformationen an den anfordernden Server-SP oder das CMM zurück.

---

**Hinweis –** Sie können die Zuweisung von Ethernet-IP-Adressen automatisch vom DHCP-Server durchführen lassen oder den DHCP-Server so konfigurieren, dass bestimmte Ethernet-IP-Adressen zugewiesen werden, indem Sie die MAC-Adresse des SP angeben. Weitere Informationen hierzu finden Sie in der Benutzerdokumentation des DHCP-Servers. Weitere Informationen zum Abrufen der MAC-Adresse des Server-SP oder CMM finden Sie unter „MAC-Adresse der SP-Netzwerkschnittstelle“ auf Seite 16.

---

## Voraussetzungen für die Zuweisung über DHCP

Folgende Bedingungen müssen erfüllt sein, damit den Server-SP-Schnittstellen IP-Adressen über einen DHCP-Server zugewiesen werden können:

- Am Serververwaltungsanschluss oder CMM-Verwaltungsanschluss muss ein Ethernet-Kabel angeschlossen sein.
- Ein DHCP-Server muss eine Verbindung mit demselben Teilnetz unterhalten wie die Serverplattform.
- Der DHCP-Server muss so konfiguriert sein, dass neue MAC-Adressen (Media Access Control) akzeptiert werden.
- Die DHCP-Konfigurationseinstellung in ILOM muss aktiviert sein. Diese Einstellung ist standardmäßig aktiviert.

## MAC-Adresse der SP-Netzwerkschnittstelle

Wen Sie beabsichtigen, der SP-Netzwerkschnittstelle eine IP-Adresse über einen DHCP-Server zuzuweisen, benötigen Sie möglicherweise die MAC-Adresse des Server-SP oder CMM.

Die MAC-Adresse des Service-Prozessors können Sie mithilfe einer der in TABELLE 2-2 beschriebenen Methoden abrufen.

**TABELLE 2-2** Methoden zum Abrufen der SP-MAC-Adresse

| ILOM-Kategorie | Methode | Beschreibung |
|---|---|---|
| Rack-System-Server-SP | Anzeigen der internen Bezeichnung | Normalerweise steht die MAC-Adresse für den Server-SP im Verwaltungsnetzwerk auf einem Klebeetikett, das am Server angebracht ist. |
| Blade-Server-SP | | Wenn die MAC-Adresse nicht auf einem am Server angebrachten Klebeetikett steht, sehen Sie in der Benutzerdokumentation nach, die der jeweiligen Serverplattform beiliegt. |
| CMM | Anzeigen der internen Bezeichnung | Normalerweise steht die MAC-Adresse für das CMM im Verwaltungsnetzwerk auf einem Klebeetikett, das am CMM angebracht ist. |
| | | Wenn die MAC-Adresse nicht auf einem am CMM angebrachten Klebeetikett steht, sehen Sie in der Benutzerdokumentation nach, die der jeweiligen Serverplattform beiliegt. |
| Alle | Kundeninformationsblatt | Sehen Sie im Kundeninformationsblatt nach, das der jeweiligen Serverplattform beiliegt. |

## Anforderungen nach der Zuweisung über DHCP

Nachdem der SP-Netzwerkschnittstelle eine IP-Adresse vom DHCP-Server zugewiesen wurde, können die vom DHCP-Server zugewiesenen IP-Adressen mithilfe einer der in TABELLE 2-3 angegebenen Methoden identifiziert werden.

**TABELLE 2-3** Methoden zum Identifizieren der vom DHCP-Server zugewiesenen IP-Adressen

| Methode | Beschreibung |
|---|---|
| DHCP-Protokolldatei<br><br>(Beachten Sie, dass diese Protokolldatei nicht Bestandteil von ILOM ist. Es handelt sich um die Protokolldatei auf dem DHCP-Server.) | Öffnen Sie die DHCP-Protokolldatei und gehen Sie wie folgt vor:<br>1. Suchen Sie die MAC-Adresse des Service-Prozessors im MAC-Adressenfeld (MAC Address).<br>2. Suchen Sie den im IP-Adressenfeld (IP Address) zugewiesenen IP-Wert, der der MAC-Adresse im MAC-Adressenfeld entspricht.<br>3. Verwenden Sie die in Schritt 2 identifizierte IP-Adresse, um eine entfernte Verbindung mit ILOM über die Webbenutzeroberfläche herzustellen.<br>**Tipp**. Normalerweise stehen DHCP-Protokolldateieinträge jeweils auf einer eigenen Zeile und enthalten die folgenden durch Kommas getrennten Felder: ID, Date, Time, Description, IP Address, Host Name, MAC Address. |
| Serielle Konsolenverbindung | Stellen Sie eine serielle Konsolenverbindung am seriellen Anschluss des Servers oder des CMM her.<br>Melden Sie sich mithilfe der CLI bei ILOM als root-Benutzer an, und geben Sie einen der folgenden Befehle ein:<br>• Bei Rack-System-Standalone-Servern: `show /SP/network`<br>• Bei einem Blade-Server-Gehäusemodul: `show /CH/BLn/SP network`<br>• Bei einem Gehäuse-CMM in Steckplatz 0: `show /CMM/network/CMM0`<br>• Bei einem Gehäuse-CMM in Steckplatz 1: `show /CMM/network/CMM1` |

# Aspekte bei der Zuweisung statischer IPs

Wen Sie beabsichtigen, einem Server-SP oder CMM statische IP-Adressen zuzuweisen, finden Sie Informationen hierzu in folgenden Themen:

- „Voraussetzungen für die Zuweisung statischer IP-Adressen“ auf Seite 18
- „Einstellungen des seriellen Geräts bzw. der Terminalemulationssoftware“ auf Seite 19
- „Nach der Zuweisung statischer IP-Adressen“ auf Seite 19

# Voraussetzungen für die Zuweisung statischer IP-Adressen

Für die erste Zuweisung einer statischen IP-Adresse zu einem Server-SP oder CMM müssen die in TABELLE 2-4 beschriebenen Voraussetzungen erfüllt sein.

**TABELLE 2-4** Voraussetzungen für die Zuweisung statischer IP-Adressen

| Voraussetzungen | Schritt | Beschreibung |
|---|---|---|
| Herstellen einer seriellen Konsolenverbindung | 1 | Stellen Sie eine serielle Konsolenverbindung mit dem Server-SP oder CMM her, indem Sie ein Terminal oder einen Computer, auf dem eine Terminalemulationssoftware ausgeführt wird, am seriellen Anschluss eines Servers oder CMM anschließen.<br>Weitere Informationen zum Anschließen eines seriellen Terminals oder eines Computers am seriellen Anschluss eines Servers oder CMM finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.<br>Beachten Sie, dass Sie bei Serverplattformen, die mit einem CMM ausgestattet sind, die statische IP-Adresse für die Blade-SPs, die im Gehäuse installiert sind, mithilfe der ILOM-CLI des CMM konfigurieren können. |
| Konfigurieren der Einstellungen des seriellen Anschlusses | 2 | Konfigurieren Sie die erforderlichen seriellen Einstellungen für das Terminalgerät oder die Terminalemulationssoftware.<br>Weitere Informationen zu diesem Thema finden Sie unter „Einstellungen des seriellen Geräts bzw. der Terminalemulationssoftware“ auf Seite 19. |
| Zuweisen der statischen IP-Adresse mithilfe der ILOM-CLI | 3 | Weisen Sie die statische IP-Adresse mithilfe der ILOM-CLI zu.<br>Weitere Informationen erhalten Sie in folgenden, auf Ihre Systemkonfiguration zutreffenden Themen:<br>• „Zuweisen einer statischen IP-Adresse zum Server-SP mithilfe einer seriellen Verbindung“ auf Seite 25.<br>oder<br>• „Zuweisen einer statischen IP-Adresse zum CMM mithilfe einer seriellen Verbindung“ auf Seite 27. |

## Einstellungen des seriellen Geräts bzw. der Terminalemulationssoftware

Beim Herstellen einer Verbindung mit ILOM mithilfe einer seriellen Konsole müssen Sie das Terminalgerät oder die Terminalemulationssoftware so konfigurieren, dass folgende serielle Einstellungen verwendet werden:

- 8N1: acht Daten-Bits, keine Parität, ein Stopp-Bit
- 9600 Baud
- Hardwareflusssteuerung deaktivieren (CTS/RTS)
- Softwareflusssteuerung deaktivieren (XON/XOFF)

Die folgenden `show`-Befehle der CLI ermöglichen das Anzeigen von Eigenschaften und Werten, die dem externen seriellen Anschluss eines Servers oder CMM zugeordnet sind:

```
show <Ziel>
```

Beispiele:

- Bei einem CMM: `show /CMM/serial/external`
- Bei einem Rack-System-Server: `show /SP/serial/external`
- Bei einem Blade-Servermodul: `show /CH/BLn/SP/serial/external`

## Nach der Zuweisung statischer IP-Adressen

IP-Adressen können mithilfe der ILOM-Webbenutzeroberfläche oder -CLI entfernt verwaltet werden, nachdem die folgenden Anforderungen erfüllt sind:

- Einem Server-SP oder CMM wurden IP-Adressen zugewiesen.
- Mit dem Server- oder CMM-Netzwerkverwaltungsanschluss wurde eine Ethernet-Verbindung hergestellt.

Weitere Information zum Verwalten der Zuweisung von IP-Adressen mithilfe einer Ethernet-Netzwerkverwaltungsverbindung finden Sie unter „Bearbeiten von IP-Adressenzuweisungen mithilfe einer Ethernet-Verwaltungsverbindung“ auf Seite 29.

# Konfiguration von Verwaltungsnetzwerk-IP-Adressen

IP-Verbindungen von ILOM sind normalerweise auf die SP-Netzwerkschnittstelle konfiguriert, wodurch eine Trennung des Verwaltungsverkehrs vom Datenverkehr erfolgen kann. Die einem Server-SP oder CMM über DHCP oder statisch zugewiesenen IP-Adressen werden auch als *Verwaltungsnetzwerk-IP-Adressen* bezeichnet. Diese sind nicht mit den Datennetzwerk-IP-Adressen zu verwechseln.

Beachten Sie, dass die Datennetzwerk-IP-Adressen erst nach der Installation eines Hostbetriebssystems auf einem Server konfiguriert werden. Es ist wichtig, zwischen den Datennetzwerk-IP-Adressen und den Verwaltungsnetzwerk-IP-Adressen zu unterscheiden, da sie sehr unterschiedlichen Zwecken dienen.

Im weiteren Verlauf des Handbuchs werden die Verwaltungsnetzwerk-IP-Adressen nur noch als „IP-Adresse des Server-SP“ oder „IP-Adresse des CMM“ bezeichnet. Normalerweise tauchen diese Bezugnahmen auf, wenn Anweisungen zum Herstellen einer Verbindung mit der ILOM-Webbenutzeroberfläche oder der ILOM-CLI gegeben werden.

Weitere Informationen zum Verwaltungsnetzwerk von ILOM finden Sie unter „ILOM-Verwaltungsnetzwerk“ auf Seite 4.

Informationen zum Zuweisen von Datennetzwerk-IP-Adressen zu einem Server finden Sie in der Benutzerdokumentation, die dem Hostbetriebssystem beiliegt.

# Zuweisen von ILOM-Netzwerkanschlüssen

In TABELLE 2-5 und TABELLE 2-6 werden die Standardnetzwerkanschlüsse angegeben, die von ILOM verwendet werden. Die meisten dieser Netzwerkanschlüsse können konfiguriert werden. Beim Konfigurieren des Firewallsicherheitszugriffs auf ILOM müssen Sie diese Anschlüsse mit den entsprechenden Werten konfigurieren, die aktuell vom Firewalldienst verwendet werden.

**TABELLE 2-5** Direkte Server-SP-Zuweisung von ILOM-Anschlüssen

| Anschlüsse | Protokolle | Anwendungen |
|---|---|---|
| 80 | HTTP über TCP | SP - konfigurierbarer ILOM-Anschluss |
| 443 | HTTPS über TCP | SP - konfigurierbarer ILOM-Anschluss |
| 5120 | TCP | SP - ILOM-Remotekonsole: CD |
| 5123 | TCP | SP - ILOM-Remotekonsole: Diskette |
| 5121 | TCP | SP - ILOM-Remotekonsole: Tastatur und Maus |

**TABELLE 2-5** Direkte Server-SP-Zuweisung von ILOM-Anschlüssen *(Fortsetzung)*

| | | |
|---|---|---|
| 7578 | TCP | SP - ILOM-Remotekonsole: Bildschirmanzeige |
| 22 | SSH über TCP | SSH - Secure Shell |
| 69 | TFTP über UDP | TFTP - Trivial File Transfer Protocol |
| 123 | NTP über UDP | NTP - Network Time Protocol |
| 161 | SNMP über UDP | SNMP - Simple Network Management Protocol |
| 162 | IPMI über UDP | IPMI - PET (Platform Event Trap) (ausgehender Anschluss) |
| 389 | LDAP über UDP/TCP | LDAP - Lightweight Directory Access Protocol (konfigurierbarer Anschluss) |
| 514 | Syslog über UDP | Syslog - (ausgehender Anschluss) |
| 546 | DHCP über UDP | DHCP - Dynamic Host Configuration Protocol (Client) |
| 623 | IPMI über UDP | IPMI - Intelligent Platform Management Interface |
| 1812 | RADIUS über UDP | RADIUS - Remote Authentication Dial In User Service (DFÜ-Benutzerdienst mit entfernter Authentifizierung) |

**TABELLE 2-6** Direkte CMM-Zuweisung von ILOM-Netzwerkanschlüssen

| Anschlüsse | Protokolle | Anwendungen |
|---|---|---|
| 80 | HTTP über TCP | CMM - ILOM (konfigurierbarer Anschluss) |
| 443 | HTTPS über TCP | CMM - ILOM (konfigurierbarer Anschluss) |
| 8000 - 8009 | HTTP über TCP | CMM - ILOM Detailebenen (BL0-BL9) |
| 8400 - 8409 | HTTPS über TCP | CMM - ILOM Detailebenen (BL0-BL9) |
| 22 | SSH über TCP | SSH - Secure Shell |
| 69 | TFTP über UDP | TFTP - Trivial File Transfer Protocol |
| 123 | NTP über UDP | NTP - Network Time Protocol |
| 161 | SNMP über UDP | SNMP - Simple Network Management Protocol |
| 389 | LDAP über UDP/TCP | LDAP - Lightweight Directory Access Protocol (konfigurierbarer Anschluss) |
| 514 | Syslog über UDP | Syslog - (ausgehender Anschluss) |
| 546 | DHCP über UDP | DHCP - Dynamic Host Configuration Protocol (Client) |
| 1812 | RADIUS über UDP | RADIUS - Remote Authentication Dial In User Service (DFÜ-Benutzerdienst mit entfernter Authentifizierung) |

# Hostnamenkennung für Server-SP und CMM

Alternativ zu einer IP-Adresse kann ein bestimmter Server-SP oder ein CMM im Netzwerk auch über einen Hostnamen identifiziert werden. Mithilfe des Hostnamens kann auch eine Verbindung mit dem Server-SP ILOM oder CMM ILOM hergestellt werden. Normalerweise müssen Sie bei diesem Typ von Systemkennung und -verbindung im verwendeten Dienst für die Namensauflösung (z. B. DNS, NIS, SMB) den Hostnamen einer IP-Adresse des Server-SP (oder CMM) zuordnen. Wenn Sie in Ihrer Netzwerkumgebung Hostnamen zur Identifizierung von Server-SPs bzw. CMMs verwenden, können Sie optional dieselbe Identifizierung in ILOM für einen Server-SP oder CMM verwenden, indem Sie den Hostnamen des Server-SP (oder CMM) auf der Seite System Identification eingeben. Weitere Informationen hierzu finden Sie unter „Zuweisen von Hostnamen oder Systemkennungen mithilfe der Webbenutzeroberfläche“ auf Seite 33.

# Systemkennungs-Textzeichenfolgen für Server

Die Systemkennung ist eine Textzeichenfolge, die Sie festlegen können, um damit Komponenten eines Systems leichter identifizieren zu können. Beispielsweise können Sie eine Systemkennung erstellen, die den Standort eines Systems, z. B. einen bestimmten Server in einem Rack, oder Details zum Zweck eines Systems angibt.

Systemkennungen sind ebenfalls in SNMP-Traps enthalten. Systemkennungen können Ihnen dabei helfen, die Trap der betreffenden ILOM-Instanz zuzuordnen, die auf dem System ausgeführt wird.

Wenn in ILOM eine Systemkennung festgelegt wird, können alle Textzeichen außer Anführungszeichen zum Beschreiben des Systems oder der Komponente verwendet werden. Weitere Informationen zum Angeben einer Systemkennung in ILOM finden Sie unter „Zuweisen von Hostnamen oder Systemkennungen“ auf Seite 33.

# Zuweisen von IP-Adressen zu den Serverplattform-SP-Schnittstellen

Mithilfe der folgenden Verfahren können Sie den SP-Netzwerkschnittstellen auf einer Serverplattform IP-Adressen zuweisen:


- „Zuweisen von IP-Adressen über DHCP mithilfe einer Ethernet-Verwaltungsverbindung“ auf Seite 23
- „Zuweisen einer statischen IP-Adresse zum Server-SP mithilfe einer seriellen Verbindung“ auf Seite 25
- „Zuweisen einer statischen IP-Adresse zum CMM mithilfe einer seriellen Verbindung“ auf Seite 27
- „Zuweisen von Hostnamen oder Systemkennungen mithilfe der Webbenutzeroberfläche“ auf Seite 33
- „Zuweisen von Hostnamen oder Systemkennungen mithilfe der CLI“ auf Seite 34


## ▼ Zuweisen von IP-Adressen über DHCP mithilfe einer Ethernet-Verwaltungsverbindung

Führen Sie diese Schritte durch, um IP-Adressen über DHCP zuzuweisen:

1. **Stellen Sie sicher, dass der DHCP-Server so konfiguriert ist, dass neue MAC-Adressen (Media Access Control) akzeptiert werden.**

   Ziehen Sie die Dokumentation heran, die der DHCP-Serversoftware beiliegt.

2. **Vergewissern Sie sich, dass ein Ethernet-Kabel an einen der folgenden Anschlüsse angeschlossen ist:**
   - Ethernet-Anschluss (NET MGT) am CMM, falls zutreffend
   - Ethernet-Anschluss (MGT) an einem Rack-System-Standalone-Server, falls zutreffend

**Hinweis –** Unter der Voraussetzung, dass ILOM nicht zuvor mit einer statischen IP-Adresse konfiguriert wurde, sendet ILOM automatisch ein DHCPDISCOVER-Paket mit der ID seiner MAC-Adressen der SP-Netzwerkschnittstellen. Wurde ILOM zuvor mit einer statischen IP-Adresse konfiguriert, müssen Sie die Einstellung der statischen IP-Adresse auf der Registerkarte Network Settings deaktivieren. Weitere Informationen zum Bearbeiten von IP-Adresseinstellungen finden Sie unter „Bearbeiten von IP-Adressenzuweisungen mithilfe einer Ethernet-Verwaltungsverbindung“ auf Seite 29.

3. **Der DHCP-Server im Netzwerk gibt das DHCPOFFER-Paket mit der IP-Adresse und weiteren Informationen zurück. Der Service-Prozessor verwaltet dann die „Ausleihe“ (lease) der vom DHCP-Server zugewiesenen IP-Adressen.**
4. **Mithilfe einer der folgenden Methoden können Sie die den SP-Netzwerkschnittstellen über DHCP zugewiesenen IP-Adressen abrufen:**
   - **ILOM-CMM mithilfe einer seriellen Verbindung.**

     Anmelden als Administrator bei ILOM mithilfe einer seriellen Konsole, die an der Rückseite des CMM angeschlossen ist. So könnten Sie beispielsweise an der Anmelde-Eingabeaufforderung den vorkonfigurierten Administrator-Benutzernamen `root` mit dem dazugehörigen Standardpasswort `changeme` eingeben und dann die Eingabetaste drücken.
   - Geben Sie Folgendes ein, um das Arbeitsverzeichnis für das aktive CMM festzulegen:

     **`cd /CMM/network/CMM0`**
   - Geben Sie zum Anzeigen der aktiven CMM-IP-Adresse Folgendes ein: **`show`**
   - Geben Sie Folgendes ein, um Detailebenen und somit die IP-Adressen jedes Blades anzuzeigen:

     **`show /CH/BL0/SP/network`**

**Hinweis –** CMM0 steht für das in Steckplatz CMM0 installierte CMM. BL0 steht für den in Steckplatz BL0 installierten Blade. Um das Ziel-CMM bzw. den Ziel-Blade anzugeben, müssen Sie die Nummer des Steckplatzes angeben, in dem das Modul installiert ist. Blade-Steckplätze sind von 0 bis 9 nummeriert; CMM-Steckplätze von 0 bis 1.

   - **ILOM-Server-SP mithilfe einer seriellen Verbindung.**

     Anmelden als Administrator bei ILOM mithilfe einer seriellen Konsole, die an der Vorderseite eines Blades angeschlossen ist. So könnten Sie beispielsweise an der Anmelde-Eingabeaufforderung den vorkonfigurierten Administrator-Benutzernamen `root` mit dem dazugehörigen Standardpasswort `changeme` eingeben und dann die Eingabetaste drücken.

     Geben Sie zum Anzeigen der Blade-SP-IP-Adresse Folgendes ein:

     **`show /SP/network`**

- **DHCP-Serverprotokolle**

  Weitere ausführliche Informationen hierzu finden Sie unter „Anforderungen nach der Zuweisung über DHCP“ auf Seite 17 oder in der Benutzerdokumentation des DHCP-Servers.

## ▼ Zuweisen einer statischen IP-Adresse zum Server-SP mithilfe einer seriellen Verbindung

Führen Sie diese Schritte durch, um einem Server-SP mithilfe einer seriellen Verbindung eine statische IP-Adresse zuzuweisen:

1. **Stellen Sie eine lokale serielle Konsolenverbindung mit dem Server-SP her.**

   Schließen Sie eine serielle Konsole am seriellen Anschluss des Servers oder des CMM an. Weitere Informationen finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

2. **Konfigurieren Sie die folgenden Einstellungen im Terminalfenster, das an der angeschlossenen seriellen Konsole angezeigt wird:**
   - 8N1: acht Daten-Bits, keine Parität, ein Stopp-Bit
   - 9600 Baud
   - Hardwareflusssteuerung deaktivieren (CTS/RTS)
   - Softwareflusssteuerung deaktivieren (XON/XOFF)

3. **Drücken Sie die Eingabetaste, um eine Verbindung zwischen der seriellen Konsole und der SP-Schnittstelle herzustellen.**

   Danach wird die Anmelde-Eingabeaufforderung von ILOM angezeigt.

   Beispiel: *Hostname* `Login:`

4. **Melden Sie sich bei ILOM als Administrator an, indem Sie einen Administrator-Benutzernamen mit dazugehörigem Passwort eingeben und dann die Eingabetaste drücken.**

---

**Hinweis –** Sie können sich bei ILOM mithilfe des vorkonfigurierten Administratorkontos anmelden, das zum Lieferumfang von ILOM gehört: `root/changeme`. Weitere ausführliche Informationen hierzu finden Sie unter „Vorkonfiguriertes ILOM-Administratorkonto“ auf Seite 6.

---

Die Standardeingabeaufforderung wird angezeigt (->). Das System ist jetzt zum Empfangen von CLI-Befehlen bereit, um Netzwerkeinstellungen vorzunehmen.

5. **Geben Sie folgenden Befehl ein, um das Arbeitsverzeichnis festzulegen:**

   **`cd /SP/network`**

6. **Geben Sie mithilfe der folgenden CLI-Befehl die IP-, NetMask- und Gateway-Adresse an.**

| Befehl | Beschreibung und Beispiel |
|---|---|
| `set pendingipaddress=` | Geben Sie diesen Befehl gefolgt von der statischen IP-Adresse ein, die dem Server-SP zugewiesen werden soll.<br><br>Beispielsweise weist die Eingabe von:<br>`set pendingipaddress=129.144.82.26`<br>ILOM an, dem Server-SP `129.144.82.26` als IP-Adresse zuzuweisen. |
| `set pendingipnetmask=` | Geben Sie diesen Befehl gefolgt von der statischen NetMask-Adresse ein, die dem Server-SP zugewiesen werden soll.<br><br>Beispielsweise weist die Eingabe von:<br>`set pendingipnetmask=255.255.255.0` ILOM an, dem Server-SP `255.255.255.0` als NetMask-Adresse zuzuweisen. |
| `set pendingipgateway=` | Geben Sie diesen Befehl gefolgt von der statischen Gateway-Adresse ein, die dem Server-SP zugewiesen werden soll.<br><br>Beispielsweise weist die Eingabe von:<br>`set pendingipgateway=129.144.82.254` ILOM an, dem Server-SP `129.144.82.254` als Gateway-Adresse zuzuweisen. |
| `setpendingipdiscovery=` | Geben Sie den folgenden Befehl ein, um ILOM anzuweisen, für den Server-SP eine statische IP-Adresse festzulegen.<br><br>`set pendingipdiscovery=static` |
| `set commitpending=true` | Geben Sie diesen Befehl (`true`) ein, um die angegebenen Netzwerkeinstellungen zuzuweisen.<br><br>Beispiel:<br>`set pendingipaddress=129.144.82.26`<br>`set pendingipnetmask=255.255.255.0`<br>`set pendingipnetmask=129.144.82.254`<br>`set commitpending=true` |

Normalerweise kommt es nach dem Zuweisen (oder Ändern) einer IP-Adresse bei der ILOM-Verbindung, die mit der vorherigen IP-Adresse hergestellt wurde, zu einer Zeitüberschreitung. Verwenden Sie die neu zugewiesene IP-Adresse, um eine Verbindung mit ILOM herzustellen.

## ▼ Zuweisen einer statischen IP-Adresse zum CMM mithilfe einer seriellen Verbindung

Führen Sie diese Schritte durch, um einem CMM mithilfe einer seriellen Verbindung eine statische IP-Adresse zuzuweisen:

1. **Vergewissern Sie sich, dass die serielle Verbindung mit einem aktiven CMM funktioniert.**

   Informationen zum Anschließen einer seriellen Konsole an ein CMM finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

2. **Melden Sie sich bei ILOM als Administrator an, indem Sie einen Administrator-Benutzernamen mit dazugehörigem Passwort eingeben und dann die Eingabetaste drücken.**

---

**Hinweis –** Sie können sich bei ILOM mithilfe des vorkonfigurierten Administratorkontos anmelden, das zum Lieferumfang von ILOM gehört: `root/changeme`. Weitere ausführliche Informationen hierzu finden Sie unter „Vorkonfiguriertes ILOM-Administratorkonto“ auf Seite 6.

---

Die Standardeingabeaufforderung wird angezeigt (->), und das System ist jetzt zum Ausführen der CLI-Befehle bereit, um Netzwerkeinstellungen vorzunehmen.

3. **Geben Sie zum Festlegen einer statischen IP-Adresse für das CMM über die ILOM-CLI den folgenden Befehl ein, mit dem das Arbeitsverzeichnis festgelegt wird:**

   ```
   cd /CMM/network/CMM0
   ```

---

**Hinweis –** CMM0 bezieht sich auf das in Steckplatz CMM0 installierte CMM. Das Ziel-CMM wird durch Verweis auf die Steckplatznummer des CMM angegeben.

---

**4. Geben Sie mithilfe der folgenden Befehle die IP-, NetMask- und Gateway-Adresse an.**

| Befehl | Beschreibung und Beispiel |
|---|---|
| `set pendingipaddress=` | Geben Sie diesen Befehl gefolgt von der statischen IP-Adresse ein, die dem CMM zugewiesen werden soll.<br><br>Beispielsweise weist die Eingabe von: `set pendingipaddress=129.144.82.26` ILOM an, `129.144.82.26` als CMM-IP-Adresse zuzuweisen. |
| `set pendingipnetmask=` | Geben Sie diesen Befehl gefolgt von der statischen NetMask-Adresse ein, die dem CMM zugewiesen werden soll.<br><br>Beispielsweise weist die Eingabe von: `set pendingipnetmask=255.255.255.0` ILOM an, `255.255.255.0` als CMM-NetMask-Adresse zuzuweisen. |
| `set pendingipgateway=` | Geben Sie diesen Befehl gefolgt von der statischen Gateway-Adresse ein, die dem CMM zugewiesen werden soll.<br><br>Beispielsweise weist die Eingabe von:<br>`set pendingipgateway=129.144.82.254`ILOM an, `129.144.82.254` als CMM-Gateway-Adresse zuzuweisen. |
| `set pendingipdiscovery=` | Geben Sie den folgenden Befehl ein, um ILOM mitzuteilen, dass eine statische IP-Adresse festgelegt werden soll.<br>`set pendingipdiscovery=static` |
| `set commitpending=true` | Geben Sie diesen Befehl (`true`) ein, um die angegebenen Netzwerkeinstellungen zuzuweisen.<br><br>Beispiel:<br>`set pendingipaddress=129.144.82.26`<br>`set pendingipnetmask=255.255.255.0`<br>`set pendingipgateway=129.144.82.254`<br>`set comitpending=true` |

Wenn Sie über eine entfernte SSH-Verbindung mit ILOM verbunden sind, kommt es bei der ILOM-Verbindung, die mit der vorherigen IP-Adresse hergestellt wurde, zu einer Zeitüberschreitung. Verwenden Sie die neu zugewiesene IP-Adresse, um eine Verbindung mit ILOM herzustellen.

# Bearbeiten von IP-Adressenzuweisungen mithilfe einer Ethernet-Verwaltungsverbindung

Mithilfe der folgenden Verfahren können Sie Service-Prozessor-IP-Adressenzuweisungen über eine Ethernet-Verwaltungsverbindung verwalten:

- „Bearbeiten vorhandener IP-Adressen in ILOM mithilfe der Webbenutzeroberfläche“ auf Seite 29
- „Bearbeiten vorhandener IP-Adressen in ILOM mithilfe der CLI“ auf Seite 31

## ▼ Bearbeiten vorhandener IP-Adressen in ILOM mithilfe der Webbenutzeroberfläche

Führen Sie diese Schritte durch, um vorhandene IP-Adressen, die zuvor einem Server-SP oder CMM zugewiesen wurden, mithilfe der ILOM-Webbenutzeroberfläche zu bearbeiten:

1. **Geben Sie in einem browserbasierten Client die IP-Adresse des Server-SP oder CMM in das Adressfeld des Browsers ein, und drücken Sie die Eingabetaste.**

   Der Anmeldebildschirm von ILOM wird angezeigt.

2. **Melden Sie sich im ILOM-Anmeldebildschirm als Administrator an, indem Sie einen Administrator-Benutzernamen mit dazugehörigem Passwort eingeben.**

---

**Tipp –** Sie können sich bei ILOM mithilfe des vorkonfigurierten Administratorkontos anmelden, das zum Lieferumfang von ILOM gehört: `root/changeme`. Weitere ausführliche Informationen hierzu finden Sie unter „Vorkonfiguriertes ILOM-Administratorkonto“ auf Seite 6.

---

Die ILOM-Benutzeroberfläche wird angezeigt.

3. **Klicken Sie im rechten Teilfenster der ILOM-Benutzeroberfläche auf Configuration --> Network.**

   Die Seite Network Settings wird für den Server oder das CMM angezeigt.

**ABBILDUNG 2-1** ILOM-Server-SP – Seite Network Settings

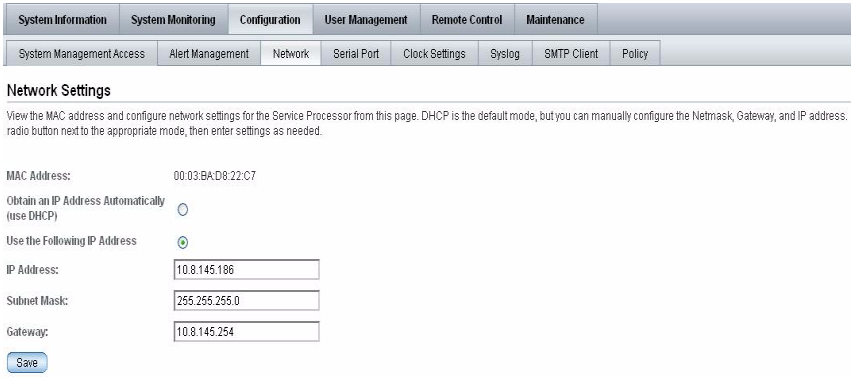
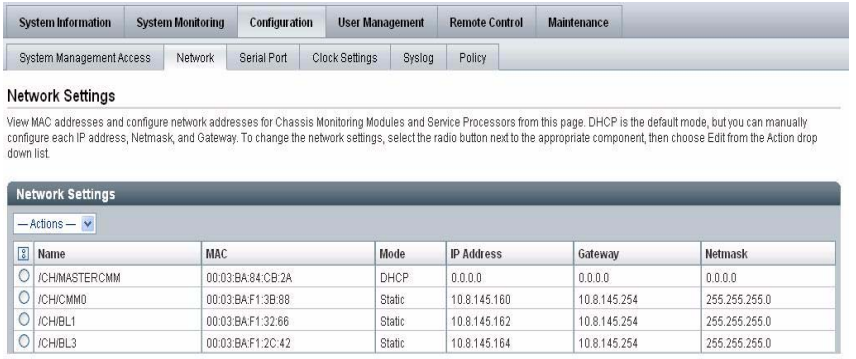



**ABBILDUNG 2-2** ILOM-CMM – Seite Network Settings




4. **Gehen Sie zum Bearbeiten von IP-Adressen, die den SP-Schnittstellen zugewiesen sind, wie folgt vor:**

   a. **Aktivieren Sie das Optionsfeld Use the Following IP Address.**

   b. **Geben Sie Werte für IP Address, Subnet Mask und Gateway in die entsprechenden Textfelder ein.**

   c. **Klicken Sie auf Save, um die neuen Einstellungen zu übernehmen.**

   Normalerweise kommt es nach dem Zuweisen (oder Ändern) einer IP-Adresse bei der ILOM-Verbindung, die mit der vorherigen IP-Adresse hergestellt wurde, zu einer Zeitüberschreitung. Verwenden Sie die neu zugewiesene IP-Adresse, um eine Verbindung mit ILOM herzustellen.

## ▼ Bearbeiten vorhandener IP-Adressen in ILOM mithilfe der CLI

Führen Sie diese Schritte durch, um vorhandene IP-Adressen, die zuvor einem Server-SP oder CMM zugewiesen wurden, mithilfe der ILOM-CLI zu bearbeiten:

1. **Stellen Sie eine lokale serielle Konsolenverbindung oder eine SSH-Verbindung mit dem Server-SP oder CMM her.**
   - **Lokale serielle Konsolenverbindung**

     Schließen Sie eine serielle Konsole am seriellen Anschluss des Servers oder des CMM an.

     Weitere Informationen finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

   oder

   - **Entfernte SSH-Verbindung (Secure Shell)**

     Stellen Sie eine SSH-Verbindung mit dem Server-SP oder CMM her.

     Stellen Sie von dem entfernten Client aus eine sichere Verbindung als root-Benutzer mit dem Server-SP oder CMM her. Sie können beispielsweise eine sichere Verbindung von einem entfernten SSH-Client aus mit dem Server-SP herstellen, indem Sie Folgendes eingeben:

     **`ssh -l root`** *server_ip_adresse*

     `Passwort:` **`changeme`**

     Die Standardeingabeaufforderung wird angezeigt (->), und das System ist jetzt zum Ausführen der CLI-Befehle bereit, um Netzwerkeinstellungen vorzunehmen.

2. **Geben Sie einen der folgenden Befehle ein, um das SP-Arbeitsverzeichnis festzulegen:**
   - Bei einem Rack-System-Standalone-Server: `cd /SP/network`
   - Bei einem Blade-Server-Gehäusemodul: `cd /SP/network`
   - Bei einem Gehäuse-CMM in Steckplatz 0: `cd /CMM/network/CMM0`
   - Bei einem Gehäuse-CMM in Steckplatz 1: `cd /CMM/network/CMM1`
3. **Geben Sie den Befehl `show` ein, um die zugewiesenen IP-Adressen anzuzeigen, beispielsweise:**
   - Bei einem Rack-System-Standalone-Server: `show /SP/network`
   - Bei einem Blade-Server-Gehäusemodul: `show /CH/BL`*n*`/SP network`
   - Bei einem Gehäuse-CMM in Steckplatz 0: `show /CMM/network/CMM0`
   - Bei einem Gehäuse-CMM in Steckplatz 1: `show /CMM/network/CMM1`

**4. Geben Sie folgende Befehle ein, um die vorhandene, zugewiesene IP-Adresse zu ändern.**

| Befehl | Beschreibung und Beispiel |
|---|---|
| `set pendingipaddress=` | Geben Sie diesen Befehl gefolgt von der statischen IP-Adresse ein, die dem Server-SP oder CMM zugewiesen werden soll.<br><br>Beispielsweise weist die Eingabe von:<br>`set pendingipaddress=129.144.82.26`<br>ILOM an, dem Server-SP `129.144.82.26` als IP-Adresse zuzuweisen. |
| `set pendingipnetmask=` | Geben Sie diesen Befehl gefolgt von der statischen NetMask-Adresse ein, die dem Server-SP oder CMM zugewiesen werden soll.<br><br>Beispielsweise weist die Eingabe von:<br>`set pendingipnetmask=255.255.255.0` ILOM an, dem Server-SP (oder CMM) `255.255.255.0` als NetMask-Adresse zuzuweisen. |
| `set pendingipgateway=` | Geben Sie diesen Befehl gefolgt von der statischen Gateway-Adresse ein, die dem Server-SP oder CMM zugewiesen werden soll.<br><br>Beispielsweise weist die Eingabe von:<br>`set pendingipgateway=129.144.82.254` ILOM an, dem Server-SP (oder CMM) `129.144.82.254` als Gateway-Adresse zuzuweisen. |
| `setpendingipdiscovery=` | Geben Sie den folgenden Befehl ein, um ILOM mitzuteilen, dass für den Server-SP oder das CMM eine statische IP-Adresse festgelegt werden soll.<br><br>`set pendingipdiscovery=static` |
| `set commitpending=true` | Geben Sie diesen Befehl (`true`) ein, um die angegebenen Netzwerkeinstellungen zuzuweisen.<br><br>Beispiel:<br>`set pendingipaddress=129.144.82.26`<br>`set pendingipnetmask=255.255.255.0`<br>`set pendingipnetmask=129.144.82.254`<br>`set commitpending=true` |

Wenn Sie über eine entfernte SSH-Verbindung mit ILOM verbunden sind, kommt es bei der ILOM-Verbindung, die mit der vorherigen IP-Adresse hergestellt wurde, zu einer Zeitüberschreitung. Verwenden Sie die neu zugewiesene IP-Adresse, um eine Verbindung mit ILOM herzustellen.

# Zuweisen von Hostnamen oder Systemkennungen

Wenn Sie zur Identifizierung von Server-SPs oder CMMs im Netzwerk Hostnamen verwenden, können Sie ILOM so konfigurieren, dass diese Identifikation (der Hostname) des Server-SP oder CMM im Banner angezeigt wird. Darüber hinaus kann ILOM mit einer aussagekräftigen Textzeichenfolge konfiguriert werden, die Ihnen die Identifizierung des Systems im Netzwerk erleichtert. Detaillierte Anweisungen zum Zuweisen eines Hostnamens oder einer Systemkennungs-Textzeichenfolge in ILOM finden Sie unter:

- „Zuweisen von Hostnamen oder Systemkennungen mithilfe der Webbenutzeroberfläche“ auf Seite 33
- „Zuweisen von Hostnamen oder Systemkennungen mithilfe der CLI“ auf Seite 34

Zusätzliche Informationen zum Zuweisen von Hostnamen oder Beispiele für Systemkennungs-Textzeichenfolgen finden Sie unter „Hostnamenkennung für Server-SP und CMM“ auf Seite 22 oder „Systemkennungs-Textzeichenfolgen für Server“ auf Seite 22.

## ▼ Zuweisen von Hostnamen oder Systemkennungen mithilfe der Webbenutzeroberfläche

Führen Sie diese Schritte durch, um in ILOM mithilfe der Webbenutzeroberfläche einen Hostnamen oder eine Systemkennung zuzuweisen:

1. **Geben Sie in einem browserbasierten Client die IP-Adresse des Server-SP in das Adressfeld des Browsers ein, und drücken Sie die Eingabetaste.**

   Das Anmeldedialogfeld von ILOM wird angezeigt.

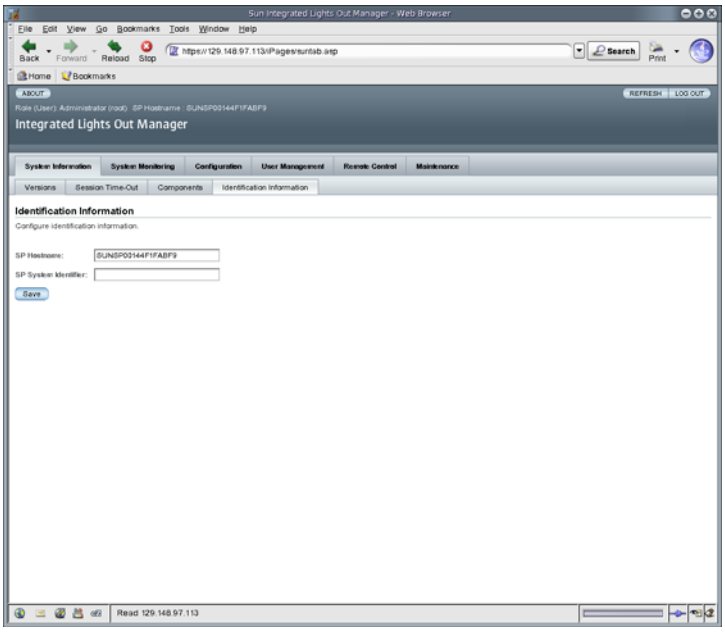
2. **Melden Sie sich im ILOM-Anmeldedialogfeld als Administrator an, indem Sie einen Administrator-Benutzernamen mit dazugehörigem Passwort eingeben.**

   Die ILOM-Benutzeroberfläche wird angezeigt.

3. **Wählen Sie System Information --> Identification Information.**

   Die Seite Identification Information wird angezeigt.

**ABBILDUNG 2-3** Seite Identification Information




4. **Geben Sie in das Feld SP Hostname den SP-Hostnamen ein.**

   Der Hostname darf aus alphanumerischen Zeichen und Bindestrichen bestehen.

5. **Geben Sie in das Feld SP System Identifier den Text ein, der für die Identifikation des Systems verwendet werden soll.**

   Die Systemkennung darf aus einer Textzeichenfolge bestehen, die alle Standardzeichen der Tastatur außer Anführungszeichen verwendet.

6. **Klicken Sie auf Save, um die neuen Einstellungen zu übernehmen.**

## ▼ Zuweisen von Hostnamen oder Systemkennungen mithilfe der CLI

Führen Sie diese Schritte durch, um in ILOM mithilfe der CLI einen Hostnamen oder eine Systemkennung zuzuweisen:

1. **Stellen Sie eine lokale serielle Konsolenverbindung oder eine SSH-Verbindung mit dem Server-SP oder CMM her.**

   - **Lokale serielle Konsolenverbindung**

     Schließen Sie eine serielle Konsole am seriellen Anschluss des Servers oder des CMM an.

Weitere Informationen finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

oder

- **Entfernte SSH-Verbindung (Secure Shell)**

  Stellen Sie eine SSH-Verbindung mit dem Server-SP oder CMM her.

  Stellen Sie von dem entfernten Client aus eine sichere Verbindung als root-Benutzer mit dem Server-SP oder CMM her. Sie können beispielsweise eine sichere Verbindung von einem entfernten SSH-Client aus mit dem Server-SP herstellen, indem Sie Folgendes eingeben:

  **ssh -l root** *server_ip_adresse*

  Passwort: **changeme**

  Die Standardeingabeaufforderung wird angezeigt (->), und das System ist jetzt zum Ausführen der CLI-Befehle bereit, um Netzwerkeinstellungen vorzunehmen.

2. **Um den SP-Hostnamen und Systemkennungstext an der Befehlseingabeaufforderung festzulegen, geben Sie Folgendes ein:**

   -> **set /SP hostname=***text_zeichenfolge*

   -> **set /SP system_identifier=***text_zeichenfolge*

   Der Hostname darf aus alphanumerischen Zeichen und Bindestrichen bestehen. Die Systemkennung darf aus einer Textzeichenfolge bestehen, die alle Standardzeichen der Tastatur außer Anführungszeichen verwendet.

KAPITEL 3

# ILOM-Befehlszeilenschnittstelle (CLI) und Anmeldung

Die ILOM-CLI (Befehlszeilenschnittstelle) ermöglicht Ihnen das Konfigurieren und Verwalten zahlreicher ILOM-Leistungsmerkmale und -Funktionen mithilfe von Tastaturbefehlen. Für jede Aufgabe, die über die ILOM-Webbenutzeroberfläche durchgeführt werden kann, ist ein entsprechender ILOM-CLI-Befehl vorhanden.

Dieses Kapitel enthält folgende Abschnitte:


- „CLI – Überblick“ auf Seite 38
- „Hierarchische CLI-Architektur“ auf Seite 38
- „CLI-Befehlssyntax“ auf Seite 40
- „Befehlsausführung“ auf Seite 42
  - „Ausführen einzelner Befehle“ auf Seite 42
  - „Ausführen kombinierter Befehle“ auf Seite 42
- „Herstellen einer Verbindung mit ILOM mithilfe der CLI“ auf Seite 43
  - „Anmelden bei ILOM“ auf Seite 43
  - „Abmelden von ILOM“ auf Seite 44


**Hinweis –** In diesem Kapitel verwendete Syntaxbeispiele verwenden das Ziel beginnend mit `/SP/`. Dies könnte in Abhängigkeit von der verwendeten Serverplattform gegen das Ziel beginnend mit `/CMM/` ausgetauscht werden. Unterziele sind auf allen Serverplattformen gleich.

# CLI – Überblick

Die ILOM-CLI basiert auf der Spezifikation Distributed Management Task Force, *Server Management Command-Line Protocol, Version 11.0a.8 Draft* (DMTF CLP). Die gesamte Spezifikation finden Sie unter folgender Adresse: `http://www.dmtf.org/standards/published_documents/DSP0214.pdf`

Die DMTF CLP stellt eine Verwaltungsschnittstelle für einen oder mehrere Server zur Verfügung, unabhängig vom Serverstatus, der Zugriffsmethode oder dem installierten Betriebssystem.

Die Architektur der DMTF CLP modelliert einen hierarchischen Namespace, eine vordefinierte Struktur, die alle verwalteten Objekte im System enthält. In diesem Modell wird ein umfangreicher Namespace mit Zielen mithilfe einer kleinen Anzahl von Befehlen, die durch Optionen und Eigenschaften geändert werden können, bearbeitet. Dieser Namespace definiert die Ziele für jedes Befehlsverb.

# Hierarchische CLI-Architektur

In der folgenden Tabelle werden die verschiedenen Hierarchiemethoden aufgeführt, die in Abhängigkeit von der verwendeten spezifischen Serverplattform mit der ILOM-CLI verwendet werden können.

**TABELLE 3-1** ILOM-Zieltypen

| Zieltyp | Beschreibung |
|---|---|
| * `/SP` | Die Ziele und Eigenschaften unterhalb dieses Zieltyps werden zum Konfigurieren des ILOM-SP (Service-Prozessor) sowie zum Anzeigen von Protokollen und Konsolen verwendet. |
| * `/CMM` | Auf Blade-Plattformen ersetzt dieser Zieltyp `/SP` und wird zum Konfigurieren des ILOM-CMM (Chassis Monitoring Module, Gehäuseüberwachungsmodul) verwendet. |
| * `/SYS` | Die Ziele und Eigenschaften unterhalb dieses Zieltyps stellen Inventar-, Umgebungs- und Hardwareverwaltung zur Verfügung. Die Ziele entsprechen unmittelbar der Nomenklatur für alle Hardwarekomponenten, von denen einige auf der physikalischen Hardware aufgedruckt sind. |

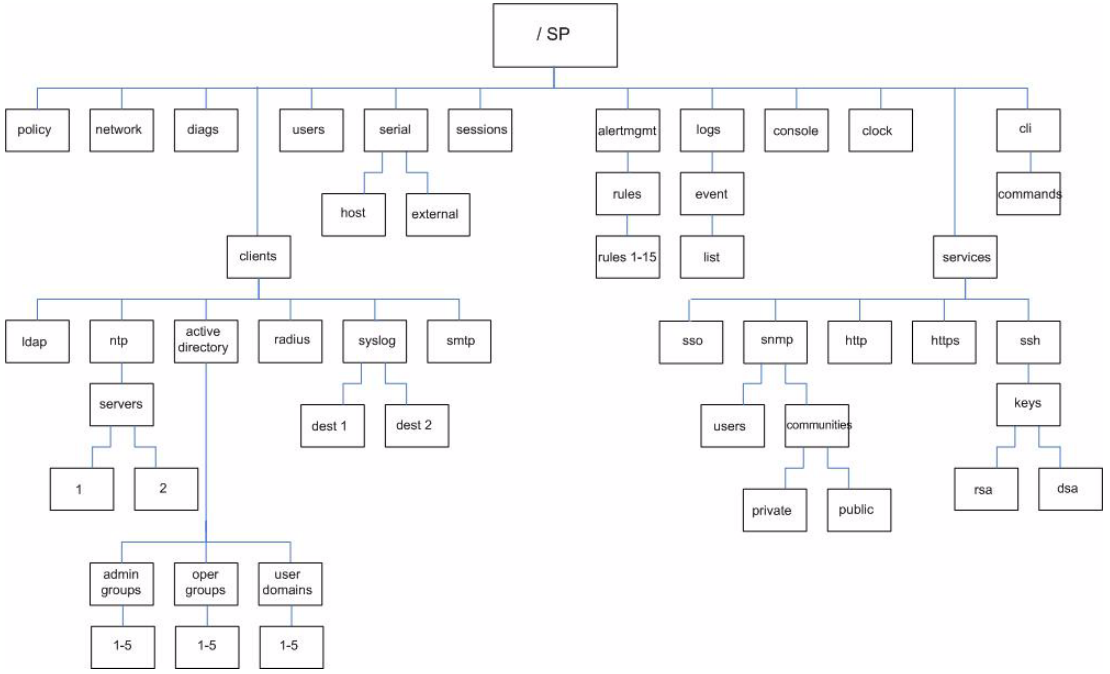
**TABELLE 3-1** ILOM-Zieltypen *(Fortsetzung)*

| Zieltyp | Beschreibung |
|---|---|
| * /CH | Auf Blade-Plattformen ersetzt dieser Zieltyp /SYS und stellt Inventar-, Umgebungs- und Hardwareverwaltung auf der Gehäuseebene zur Verfügung. Die Zieltypen entsprechen unmittelbar den Nomenklaturnamen für alle Hardwarekomponenten, von denen einige auf der physikalischen Hardware aufgedruckt sind. |
| * /HOST | Die Ziele und Eigenschaften unterhalb dieses Zieltyps werden zur Überwachung und Verwaltung des Hostbetriebssystems verwendet. Dieser ist nur für die Verwendung mit SPARC-Systemen verfügbar. |

**Hinweis –** Der Zugriff auf einige dieser Unterstrukturen innerhalb der Hierarchie ist von der verwendeten Serverplattform abhängig.

Service-Prozessoren können auf zwei Namespaces zugreifen: den Namespace /SP und den Gesamtsystem-Namespace /SYS. Im Namespace /SP kann der Service-Prozessor verwaltet und konfiguriert werden. Im Namespace /SYS kann auf Sensoren und andere Informationen für verwaltete Systemhardware zugegriffen werden.

**ABBILDUNG 3-1** /SP Beispiel für die ILOM-CLI-Zielstruktur




Informationen zu Stufen von Benutzerrechten finden Sie unter „Rollen für ILOM-Benutzerkonten“ auf Seite 6.

# CLI-Befehlssyntax

Bei Verwendung der ILOM-CLI werden Informationen in der folgenden Reihenfolge eingegeben:

Befehlssyntax: `<Befehl> <Optionen> <Ziel> <Eigenschaften>`

Die folgenden Abschnitte enthalten weitere Informationen zu den einzelnen Teilen der Syntax.

## CLI-Befehle

Die ILOM-CLI unterstützt die Befehle der DMTF CLP, die in der folgenden Tabelle aufgeführt sind.

CLI-Befehle unterscheiden zwischen Groß- und Kleinschreibung.

**TABELLE 3-2** CLI-Befehle

| Befehl | Beschreibung |
|---|---|
| `cd` | Navigiert im Objekt-Namespace. |
| `create` | Richtet ein Objekt im Namespace ein. |
| `delete` | Entfernt ein Objekt aus dem Namespace. |
| `exit` | Beendet eine CLI-Sitzung. |
| `help` | Zeigt Hilfeinformationen zu Befehlen und Zielen an. |
| `load` | Überträgt eine Datei von einer angegebenen Quelle an ein angegebenes Ziel. |
| `reset` | Setzt den Status des Ziels zurück. |
| `set` | Legt Zieleigenschaften auf den angegebenen Wert fest. |
| `show` | Zeigt Informationen zu Zielen und Eigenschaften an. |
| `start` | Startet das Ziel. |
| `stop` | Beendet das Ziel. |
| `version` | Zeigt die Version des ausgeführten Service-Prozessors an. |

# Befehlsoptionen

Die ILOM-CLI unterstützt folgende Optionen. Beachten Sie aber, dass nicht jeder Befehl alle Optionen unterstützt. Die Optionen `help` und `examine` können mit allen Befehlen verwendet werden.

**TABELLE 3-3** CLI-Optionen

| Langform der Option | Kurzform | Beschreibung |
|---|---|---|
| `-default` | | Der Befehl führt nur die Standardfunktionen aus. |
| `-destination` | | Gibt das Ziel für Daten an. |
| `-display` | `-d` | Zeigt die Daten an, die der Benutzer anzeigen möchte. |
| `-help` | `-h` | Zeigt Hilfeinformationen an. |
| `-level` | `-l` | Führt den Befehl für das aktuelle Ziel und alle Ziele aus, die aufgrund der angegebenen Ebene enthalten sind. |
| `-output` | `-o` | Gibt den Inhalt und die Form der Befehlsausgabe an. ILOM unterstützt nur `-o table`, wodurch Ziele und Eigenschaften in Tabellenform angezeigt werden. |
| `-script` | | Übergeht Warnungen oder Aufforderungen, die normalerweise dem Befehl zugeordnet sind. |
| `-source` | | Gibt die Position eines Quellabbilds an. |

# Befehlsziele

Jedes Objekt im Namespace ist ein Ziel.

# Befehlseigenschaften

Eigenschaften sind die konfigurierbaren Attribute, die spezifisch für jedes Objekt sind.

# Befehlsausführung

Für die meisten Befehle geben Sie zum Ausführen die Position des Ziels an und geben dann den Befehl ein. Diese Aktionen können einzeln oder kombiniert auf derselben Befehlszeile ausgeführt werden.

## ▼ Ausführen einzelner Befehle

1. **Navigieren Sie mithilfe des Befehls** `cd` **zum Namespace.**

   Beispiel:

   ```
   cd /SP/services/http
   ```

2. **Geben Sie den Befehl, das Ziel und den Wert ein.**

   Beispiel:

   ```
   set port=80
   ```

   oder

   ```
   set prop1=x
   set prop2=y
   ```

## ▼ Ausführen kombinierter Befehle

- **Geben Sie mithilfe der Syntax** `<Befehl><Ziel>=`*Wert* **den Befehl auf einer einzigen Befehlszeile ein.**

  Beispiel:

  ```
  set /SP/services/http port=80
  ```

  oder

  ```
  set /SP/services/http prop1=x prop2=y
  ```

Die folgende Tabelle zeigt Beispiele und Beschreibungen für die Ausführungsmethoden einzelner und kombinierter Befehle.

**TABELLE 3-4** Ausführen einzelner und kombinierter Befehle

| Befehlssyntax | Befehlsbeschreibung |
|---|---|
| Ausführen eines einzelnen Befehls:<br>`> cd /SP/services/http` | Navigiert zum Namespace `/SP/services/http` |
| `> set port=80` | Geben Sie den Befehl, das Ziel und den Wert ein:<br>Legt „port“ (Anschluss) auf „80“ fest. |
| Ausführen eines kombinierten Befehls:<br>`> cd /SP/services/http port=80` | Legt im Namespace `/SP/services/http` das Ziel „port“ (Anschluss) auf „80“ fest. |

# Herstellen einer Verbindung mit ILOM mithilfe der CLI

In diesem Abschnitt wird das An- und Abmelden bei ILOM beschrieben. Lesen Sie zuerst „Zuweisen von IP-Adressen zu den Serverplattform-SP-Schnittstellen“ auf Seite 23, um ILOM zu konfigurieren, bevor Sie sich bei der ILOM-CLI anmelden.

ILOM unterstützt maximal 10 aktive Sitzungen, einschließlich serieller, SSH- und Webbenutzeroberflächensitzungen. Telnet-Verbindungen mit ILOM werden nicht unterstützt.

## ▼ Anmelden bei ILOM

Der Zugriff auf die ILOM-CLI kann entfernt (remote) über eine SSH- (Secure Shell) oder eine serielle Verbindung erfolgen. SSH-Verbindungen sind standardmäßig aktiviert.

Das folgende Verfahren zeigt ein Beispiel für die Verwendung eines SSH-Clients auf einem UNIX-System. Verwenden Sie einen für Ihr Betriebssystem geeigneten SSH-Client. Der Standardbenutzername ist `root`, und das Standardpasswort lautet `changeme`.

Führen Sie diese Schritte durch, um sich mithilfe der standardmäßig aktivierten SSH-Verbindung bei ILOM anzumelden:

1. **Geben Sie diesen Befehl ein, um sich bei ILOM anzumelden:**

   `$` **`ssh root@`***`IPadresse`*

   wobei *IPadresse* die IP-Adresse des Server-SP ist.

2. **Geben Sie auf Aufforderung dieses Passwort ein:**

   ```
   Passwort: changeme
   ```

Nachdem Sie sich mithilfe des Standardbenutzernamens und -passworts bei ILOM angemeldet haben, müssen Sie das Passwort für das root-Konto von ILOM (`changeme`) ändern. Informationen zum Ändern des Passworts des root-Kontos finden Sie unter „Ändern des Passworts des root-Kontos in ILOM mithilfe der CLI“ auf Seite 69.

## ▼ Abmelden von ILOM

Führen Sie diesen Schritt aus, um sich bei ILOM abzumelden:

- **Geben Sie diesen Befehl ein, um sich bei ILOM abzumelden:**

  ```
  -> exit
  ```

KAPITEL 4

# ILOM-Webbenutzeroberfläche und Anmeldung

ILOM unterstützt eine einfach zu bedienende Webbenutzeroberfläche, die in zahlreichen Webbrowsern ausgeführt werden kann. Mithilfe dieser Webbenutzeroberfläche können Sie auf alle Leistungsmerkmale und Funktionen von ILOM zugreifen.

Dieses Kapitel enthält folgende Abschnitte:


- „Webbenutzeroberfläche – Überblick“ auf Seite 45
- „Anforderungen an Browser und Software“ auf Seite 46
- „Komponenten der Webbenutzeroberfläche“ auf Seite 47
- „Komponenten der Navigationsregisterkarten“ auf Seite 48
- „Herstellen einer Verbindung mit ILOM mithilfe der Webbenutzeroberfläche“ auf Seite 57
  - „Anmelden bei ILOM“ auf Seite 57
  - „Hochladen des SSL-Zertifikats“ auf Seite 60
  - „Festlegen der Sitzungszeitüberschreitung“ auf Seite 61
  - „Abmelden von ILOM“ auf Seite 62


## Webbenutzeroberfläche – Überblick

Auf die ILOM-Webbenutzeroberfläche, die eine Standardbenutzeroberfläche verwendet, kann über einen Browser zugegriffen werden. Mithilfe der ILOM-Webbenutzeroberfläche können Sie lokale und entfernte Systeme überwachen und verwalten. Eine der leistungsfähigsten Funktionen von ILOM ist die Möglichkeit zum Umleiten der grafischen Konsole des Servers auf eine lokale Workstation oder einen Laptop. Beim Umleiten der Hostkonsole können Sie die Tastatur und Maus des lokalen Systems so konfigurieren, dass sich diese wie Maus und Tastatur des Servers verhalten. Sie können darüber hinaus das Disketten- oder CD-ROM-Laufwerk des

entfernten Systems als ein virtuell an Ihr System angeschlossenes Gerät konfigurieren. Sie erhalten Zugriff auf dieses Leistungsmerkmal, indem Sie die ILOM-Remotekonsolenanwendung verwenden. Weitere Informationen zur Remotekonsole finden Sie in Kapitel 12. Die Webbenutzeroberfläche stellt Benutzerkonten mit definierten Rollen und Berechtigungen zur Verfügung. Informationen zu Berechtigungsstufen finden Sie unter „Rollen für ILOM-Benutzerkonten“ auf Seite 6.

# Anforderungen an Browser und Software

Die Webbenutzeroberfläche wurde erfolgreich mit den jüngst veröffentlichten Webbrowserversionen von Mozilla™, Firefox und Internet Explorer getestet und ist möglicherweise auch mit weiteren Webbrowsern kompatibel.

In einem Browser kann nur eine Instanz der ILOM-Webbenutzeroberfläche gestartet werden. Bei dem Versuch, mehrere Instanzen der ILOM-Webbenutzeroberfläche im selben Browser zu starten, wird nur die erste Instanz der Webbenutzeroberfläche angezeigt.

Folgende Betriebssysteme und Webbrowser sind mit ILOM kompatibel:

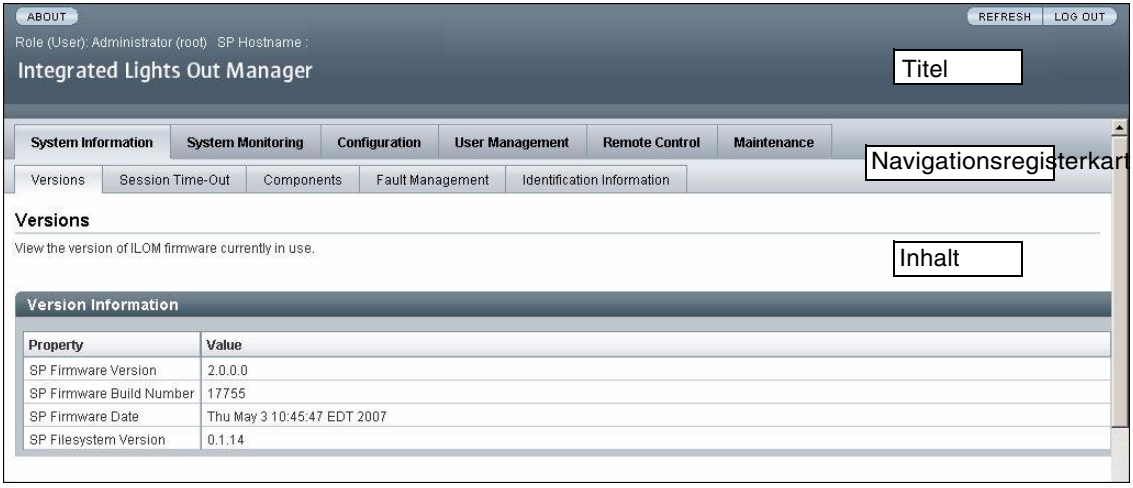
- Solaris (9 und 10)
  - Mozilla 1.4 und 1.7
  - Firefox 1.x und höher
- Linux (Red Hat, SuSE, Ubuntu)
  - Mozilla 1.x und höher
  - Firefox 1.x und höher
  - Opera 6.x und höher
- Microsoft Windows (98, 2000, XP, Vista)
  - Internet Explorer 5.5, 6.x, 7.x
  - Mozilla 1.x und höher
  - Firefox 1.x und höher
  - Opera 6.x und höher
- Macintosh (OSX v10.1 und höher)
  - Internet Explorer 5.2
  - Mozilla 1.x und höher
  - Firefox 1.x und höher
  - Safari (alle Versionen)

**Hinweis –** ILOM ist auf Ihrem System vorinstalliert und umfassst die Remotekonsolenanwendung. Zum Ausführen der ILOM-Remotekonsole muss die Java 1.5-Laufzeitumgebung (JRE 1.5) oder eine höhere Version der JRE-Software auf dem lokalen Client installiert sein. Die JRE-Software können Sie unter `http://java.com` herunterladen. Weitere Informationen zur Remotekonsole finden Sie in Kapitel 12.

# Komponenten der Webbenutzeroberfläche

Unten sehen Sie die Hauptseite der ILOM-Webbenutzeroberfläche.

**ABBILDUNG 4-1** Hauptseite der ILOM-Webbenutzeroberfläche




Jede Seite der Webbenutzeroberfläche besteht aus drei Hauptabschnitten: dem Titel, den Navigationsregisterkarten und dem Inhaltsbereich.

**Hinweis –** Bei Verwendung der ILOM-Webbenutzeroberfläche auf einem CMM (Chassis Monitoring Module) befindet sich eine weitere Komponente in der Webbenutzeroberfläche, das sogenannte Navigationsfenster.

Im Titel finden Sie auf jeder Seite der Webbenutzeroberfläche die folgenden Schaltflächen und Informationen:

- **About (Schaltfläche)** – Klicken Sie auf diese Schaltfläche, um Produkt- und Copyrightinformationen anzuzeigen.
- **Benutzerfeld** – Zeigt den Benutzernamen des aktuellen Benutzers der Webbenutzeroberfläche mit seiner Rolle an.
- **Serverfeld** – Zeigt den Hostnamen des ILOM-SP oder -CMM an.
- **Refresh (Schaltfläche)** – Klicken Sie auf diese Schaltfläche, um die Informationen im Inhaltsbereich der Seite zu aktualisieren. Durch Klicken auf die Schaltfläche Refresh werden keine neuen Daten gespeichert, die eventuell auf der Seite eingegeben oder ausgewählt wurden.
- **Log Out (Schaltfläche)** – Klicken Sie auf diese Schaltfläche, um die aktuelle Sitzung der Webbenutzeroberfläche zu beenden.

---

**Hinweis –** Verwenden Sie nicht die Schaltfläche Aktualisieren Ihres Webbrowsers, wenn Sie die Webbenutzeroberfläche verwenden.

---

Die Navigationsstruktur der ILOM-Webbenutzeroberfläche umfasst Registerkarten sowie untergeordnete Registerkarten, auf die zum Öffnen einer bestimmten Seite geklickt werden kann. Wenn Sie auf die Hauptregisterkarte klicken, werden die untergeordneten Registerkarten angezeigt, auf denen Sie weitere Optionen finden. Weitere Informationen zu diesem Thema finden Sie unter „Komponenten der Navigationsregisterkarten“ auf Seite 48.

Im Inhaltsbereich finden Sie Informationen zu dem jeweiligen spezifischen Thema oder Vorgang.

# Komponenten der Navigationsregisterkarten

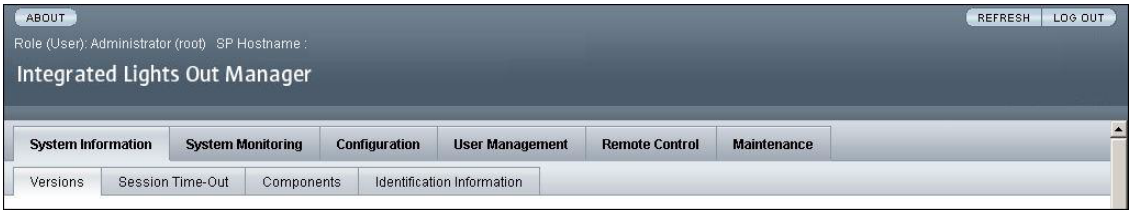
Im folgenden Abschnitt werden die verschiedenen Registerkarten mit ihren untergeordneten Registerkarten beschrieben, die Sie in den gängigsten ILOM-Komponenten in der Webbenutzeroberfläche vorfinden. Ausführlichere Informationen zu jedem dieser Bereiche finden Sie im entsprechenden Kapitel dieses Buchs.

# Registerkarte System Information

Beim Öffnen von ILOM wird standardmäßig die Registerkarte System Information mit den untergeordneten Registerkarten ähnlich der folgenden Abbildung angezeigt. Auf der Registerkarte System Information haben Sie Zugriff auf die folgenden untergeordneten Registerkarten:

- Versions (Registerkarte)
- Session Time-Out (Registerkarte)
- Components (Registerkarte)
- Identification Information (Registerkarte)

**ABBILDUNG 4-2** System Information (Registerkarte)




## Registerkarte Versions

Im Abschnitt Versions können Sie die Version von ILOM anzeigen, die ausgeführt wird. Weitere Informationen zu diesem Thema finden Sie unter „Anzeigen von ILOM-Versionsinformationen mithilfe der Webbenutzeroberfläche“ auf Seite 205.

## Registerkarte Session Time-Out

Im Abschnitt Session Time-Out können Sie den Leerlaufzeitraum festlegen, über den eine ILOM-Sitzung aktiv bleiben soll. Weitere Informationen zu diesem Thema finden Sie unter „Festlegen der Sitzungszeitüberschreitung“ auf Seite 61.

## Registerkarte Components

Im Abschnitt Components können Sie die Namen, Typen und Status der Komponenten anzeigen, die von ILOM überwacht werden. Weitere Informationen zu diesem Thema finden Sie unter „Anzeigen von Komponenteninformationen mithilfe der Webbenutzeroberfläche“ auf Seite 109.

## Registerkarte Identification Information

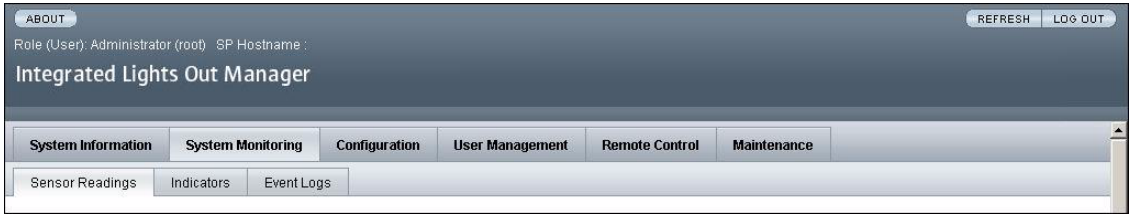
Im Abschnitt Identification Information können Sie die SP-Identifizierungsinformationen eingeben oder ändern. Weitere Informationen zu diesem Thema finden Sie unter „Zuweisen von Hostnamen oder Systemkennungen mithilfe der Webbenutzeroberfläche“ auf Seite 33.

# Registerkarte System Monitoring

Wenn Sie auf die Registerkarte System Monitoring klicken, wird die Registerkarte mit den untergeordneten Registerkarten ähnlich der folgenden Abbildung angezeigt. Auf der Registerkarte System Monitoring haben Sie Zugriff auf die folgenden untergeordneten Registerkarten:

- Sensor Readings (Registerkarte)
- Indicators (Registerkarte)
- Event Logs (Registerkarte)

**ABBILDUNG 4-3** Registerkarte System Monitoring




## Registerkarte Sensor Readings

Im Abschnitt Sensor Readings können Sie Namen, Typ und Messwerte der Sensoren anzeigen. Weitere Informationen zu diesem Thema finden Sie unter „Sensormesswerte“ auf Seite 119.

## Registerkarte Indicators

Im Abschnitt Indicators können Sie den Namen und Status der Anzeigen und LEDs anzeigen. Weitere Informationen zu diesem Thema finden Sie unter „System-LEDs“ auf Seite 123.

## Registerkarte Event Logs

Im Abschnitt Event Logs können Sie verschiedene Details zu jedem einzelnen Ereignis anzeigen, einschließlich Ereignis-ID, Klasse, Typ, Schweregrad, Datum und Zeit sowie Beschreibung des Ereignisses. Weitere Informationen zu diesem Thema finden Sie unter „ILOM-Ereignisprotokoll“ auf Seite 126.

# Registerkarte Configuration

Wenn Sie auf die Registerkarte Configuration klicken, wird die Registerkarte mit den untergeordneten Registerkarten ähnlich der folgenden Abbildung angezeigt. Auf der Registerkarte Configuration haben Sie Zugriff auf die folgenden untergeordneten Registerkarten:

- System Management Access (Registerkarte)
- Alert Management (Registerkarte)
- Network (Registerkarte)
- Serial Port (Registerkarte)
- Clock Settings (Registerkarte)
- Syslog (Registerkarte)
- SMTP Client (Registerkarte)
- Policy (Registerkarte)

**ABBILDUNG 4-4** Registerkarte Configuration

## Registerkarte System Management Access

Im Abschnitt System Management Access haben Sie Zugriff auf die Funktionen Web Server, SNMP und SSL Certificate.

### *Registerkarte Web Server*

Im Abschnitt Web Server können Sie die Webservereinstellungen bearbeiten oder aktualisieren, z. B. den HTTP-Webserver oder den HTTP-Anschluss. Weitere Informationen zu diesem Thema finden Sie unter „Aktivieren von HTTP- oder HTTPS-Webzugriff mithilfe der Webbenutzeroberfläche“ auf Seite 174.

### *Registerkarte SNMP*

Im Abschnitt SNMP können Sie SNMP-Einstellungen bearbeiten oder aktualisieren. Weitere Informationen zu diesem Thema finden Sie unter „Konfigurieren von SNMP-Einstellungen mithilfe der Webbenutzeroberfläche“ auf Seite 193.

### *Registerkarte SSL Certificate*

Im Abschnitt SSL Certificate können Sie Informationen zum SSL-Standardzertifikat anzeigen. Sie haben außerdem die Möglichkeit, ein neues SSL-Zertifikat zu suchen und einzugeben. Weitere Informationen zu diesem Thema finden Sie unter „Hochladen des SSL-Zertifikats“ auf Seite 60.

### *Registerkarte SSH Server*

Im Abschnitt SSH Server können Sie den SSH-Serverzugriff (Secure Shell) und die Schlüsselerzeugung konfigurieren. Weitere Informationen zu diesem Thema finden Sie unter „Aktivieren und Deaktivieren der SSH mithilfe der Webbenutzeroberfläche“ auf Seite 168.

## Registerkarte Alert Management

Im Abschnitt Alert Management können Sie Details zu jedem Alarm anzeigen und die Liste der konfigurierten Alarme ändern. Weitere Informationen zu diesem Thema finden Sie unter „Verwalten von Alarmregelkonfigurationen mithilfe der ILOM-Webbenutzeroberfläche“ auf Seite 145.

## Registerkarte Network

Im Abschnitt Network können Sie die Netzwerkeinstellungen für ILOM anzeigen und bearbeiten. Weitere Informationen zu diesem Thema finden Sie unter „Anzeigen von Netzwerkeinstellungen mithilfe der Webbenutzeroberfläche“ auf Seite 170.

## Registerkarte Serial Port

Im Abschnitt Serial Port können Sie die Baudrate der internen und externen seriellen Anschlüsse anzeigen und bearbeiten. Weitere Informationen zu diesem Thema finden Sie unter „Anzeigen von seriellen Anschlusseinstellungen mithilfe der Webbenutzeroberfläche“ auf Seite 172.

## Registerkarte Clock Settings

Im Abschnitt Clock Settings können Sie die Zeit- und NTP-Einstellungen anzeigen und bearbeiten. Weitere Informationen zu diesem Thema finden Sie unter „Ereignisprotokoll-Zeitstempel und ILOM-Zeiteinstellungen“ auf Seite 127.

## Registerkarte Syslog

Im Abschnitt Syslog können Sie die Serveradressen konfigurieren, an die die Syslog-Meldungen gesendet werden. Weitere Informationen zu diesem Thema finden Sie unter „Konfigurieren von IP-Adressen von entfernten Syslog-Empfängern mithilfe der Webbenutzeroberfläche“ auf Seite 139.

## Registerkarte SMTP Client

Im Abschnitt SMTP können Sie den Zustand des SMTP-Clients konfigurieren, der zum Senden von E-Mail-Benachrichtigungen für Alarme verwendet wird. Weitere Informationen zu diesem Thema finden Sie unter „Aktivieren eines SMTP-Clients mithilfe der Webbenutzeroberfläche“ auf Seite 156.

## Registerkarte Policy

Im Abschnitt Policy können Sie Einstellungen aktivieren bzw. deaktivieren, mit denen das Verhalten des Systems gesteuert wird, z. B. Einschaltrichtlinien. Weitere Informationen zu diesem Thema finden Sie unter „Konfigurieren von Richtlinieneinstellungen“ auf Seite 115.

# Registerkarte User Management

Wenn Sie auf die Registerkarte User Management klicken, wird die Registerkarte mit den untergeordneten Registerkarten ähnlich der folgenden Abbildung angezeigt. Auf der Registerkarte User Management haben Sie Zugriff auf die folgenden untergeordneten Registerkarten:

- User Accounts (Registerkarte)
- Active Sessions (Registerkarte)
- LDAP (Registerkarte)
- RADIUS (Registerkarte)
- Active Directory (Registerkarte)

**ABBILDUNG 4-5** Registerkarte User Management

## Registerkarte User Accounts

Im Abschnitt User Accounts können Sie lokale ILOM-Benutzerkonten hinzufügen, löschen und ändern. Weitere Informationen zu diesem Thema finden Sie unter „Hinzufügen von Benutzerkonten und Festlegen von Berechtigungen mithilfe der Webbenutzeroberfläche“ auf Seite 74.

## Registerkarte Active Sessions

Im Abschnitt Active Sessions können Sie die aktuell bei ILOM angemeldeten Benutzer anzeigen sowie den Typ der Sitzungen, die von Benutzern initiiert wurden. Weitere Informationen zu diesem Thema finden Sie unter „Anzeigen von Benutzersitzungen mithilfe der Webbenutzeroberfläche“ auf Seite 81.

## Registerkarte LDAP

Im Abschnitt LDAP können Sie den ILOM-Zugriff für LDAP-Benutzer konfigurieren. Weitere Informationen zu diesem Thema finden Sie unter „Konfigurieren von ILOM für LDAP mithilfe der Webbenutzeroberfläche“ auf Seite 99.

## Registerkarte RADIUS

Im Abschnitt RADIUS können Sie den ILOM-Zugriff für RADIUS-Benutzer konfigurieren. Weitere Informationen zu diesem Thema finden Sie unter „Konfigurieren von RADIUS mithilfe der Webbenutzeroberfläche“ auf Seite 102.

## Registerkarte Active Directory

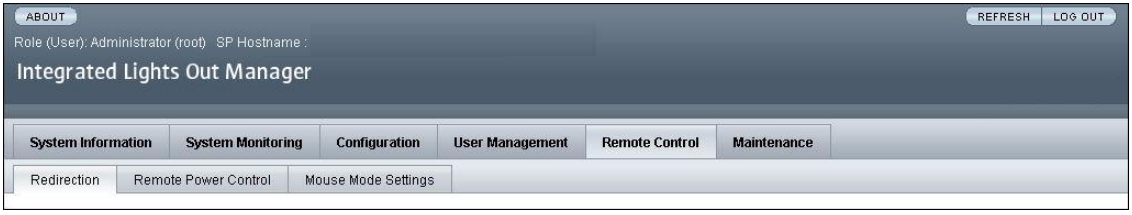
Im Abschnitt Active Directory können Sie Active Directory-Einstellungen konfigurieren. Weitere Informationen zu diesem Thema finden Sie unter „Konfigurieren von Active Directory mithilfe der Webbenutzeroberfläche“ auf Seite 83.

# Registerkarte Remote Control

Wenn Sie auf die Registerkarte Remote Control klicken, wird die Registerkarte mit den untergeordneten Registerkarten ähnlich der folgenden Abbildung angezeigt. Auf der Registerkarte Remote Control haben Sie Zugriff auf die folgenden untergeordneten Registerkarten:

- Redirection (Registerkarte)
- Remote Power Control (Registerkarte)
- Mouse Mode Settings (Registerkarte)

**ABBILDUNG 4-6** Registerkarte Remote Control




## Registerkarte Redirection

Im Abschnitt Redirection können Sie den Host entfernt verwalten, indem Sie die Systemkonsole auf Ihren lokalen Computer umleiten. Weitere Informationen zu diesem Thema finden Sie unter „Konfigurieren von ILOM-Einstellungen für entfernte Steuerung mithilfe der Webbenutzeroberfläche“ auf Seite 216.

## Registerkarte Remote Power Control

Im Abschnitt Remote Power Control können Sie die Stromversorgung des Systems steuern. Weitere Informationen zu diesem Thema finden Sie unter „Konfigurieren von ILOM-Einstellungen für entfernte Steuerung mithilfe der Webbenutzeroberfläche“ auf Seite 216.

## Registerkarte Mouse Mode Settings

Im Abschnitt Mouse Mode Settings können Sie einen Modus für die lokale Maus auswählen, der während der entfernten Verwaltung des Hosts verwendet wird. Weitere Informationen zu diesem Thema finden Sie unter „Konfigurieren von ILOM-Einstellungen für entfernte Steuerung mithilfe der Webbenutzeroberfläche“ auf Seite 216.

# Registerkarte Maintenance

Wenn Sie auf die Registerkarte Maintenance klicken, wird die Registerkarte mit den untergeordneten Registerkarten ähnlich der folgenden Abbildung angezeigt. Auf der Registerkarte Maintenance haben Sie Zugriff auf die folgenden untergeordneten Registerkarten:

- Firmware Upgrade (Registerkarte)
- Reset SP (Registerkarte)

**ABBILDUNG 4-7** Registerkarte Maintenance

### Registerkarte Firmware Upgrade

Im Abschnitt Firmware Upgrade können Sie den Prozess zum Abrufen einer Aktualisierung der ILOM-Firmware starten. Weitere Informationen zu diesem Thema finden Sie unter „Aktualisieren der ILOM-Firmware mithilfe der Webbenutzeroberfläche“ auf Seite 206.

### Registerkarte Reset SP

Im Abschnitt Reset SP können Sie den Prozess zum Zurücksetzen des Service-Prozessors (SP) starten. Weitere Informationen zu diesem Thema finden Sie unter „Zurücksetzen des ILOM-SP“ auf Seite 207.

# Herstellen einer Verbindung mit ILOM mithilfe der Webbenutzeroberfläche

In diesem Abschnitt wird das An- und Abmelden bei der Webbenutzeroberfläche beschrieben sowie das Hochladen eines SSL-Zertifikats und das Festlegen der Sitzungszeitüberschreitung.

## ▼ Anmelden bei ILOM

In diesem Abschnitt wird das Anmelden bei der ILOM-Webbenutzeroberfläche beschrieben.

---

**Hinweis –** ILOM startet automatisch, sobald ein System an eine Wechselstromversorgung angeschlossen wird bzw. wenn ein Servermodul in ein mit Strom versorgtes Gehäuse eingesetzt wird. Wenn das Verwaltungs-Ethernet nicht angeschlossen ist oder der DHCP-Prozess (Dynamic Host Configuration Protocol) von ILOM wegen eines im Verwaltungsnetzwerk fehlenden DHCP- Servers fehlschlägt, kann es länger dauern, bis ILOM startet.

---

Das Deaktivieren der Verwendung des Browserproxyservers (falls verwendet) für den Zugriff auf das Verwaltungsnetzwerk kann die Antwortzeiten der Webbenutzeroberfläche verkürzen.

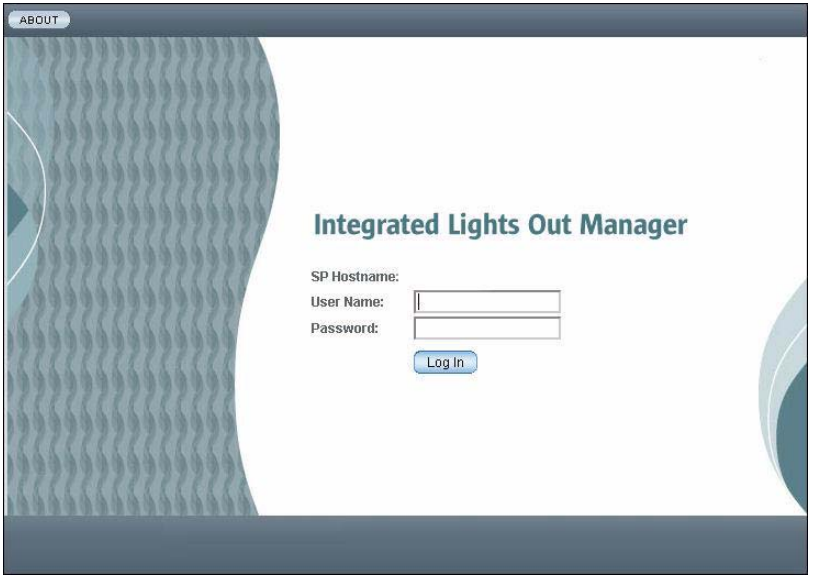
Sie benötigen die IP-Adresse von ILOM. Weitere Informationen zum Anzeigen und Festlegen der IP-Adresse finden Sie unter „Zuweisen von IP-Adressen zu den Serverplattform-SP-Schnittstellen“ auf Seite 23.

Führen Sie diese Schritte durch, um sich bei der ILOM-Webbenutzeroberfläche anzumelden:

1. **Geben Sie zum Anmelden bei der Webbenutzeroberfläche die IP-Adresse von ILOM im Webbrowser ein.**

   Die Seite Login der Webbenutzeroberfläche wird angezeigt.

**ABBILDUNG 4-8** Seite Login




2. **Geben Sie Ihren Benutzernamen und Ihr Passwort ein.**

   Sie können den Standardbenutzernamen mit Passwort verwenden.

- Standardbenutzername – `root`
- Standardpasswort – `changeme`

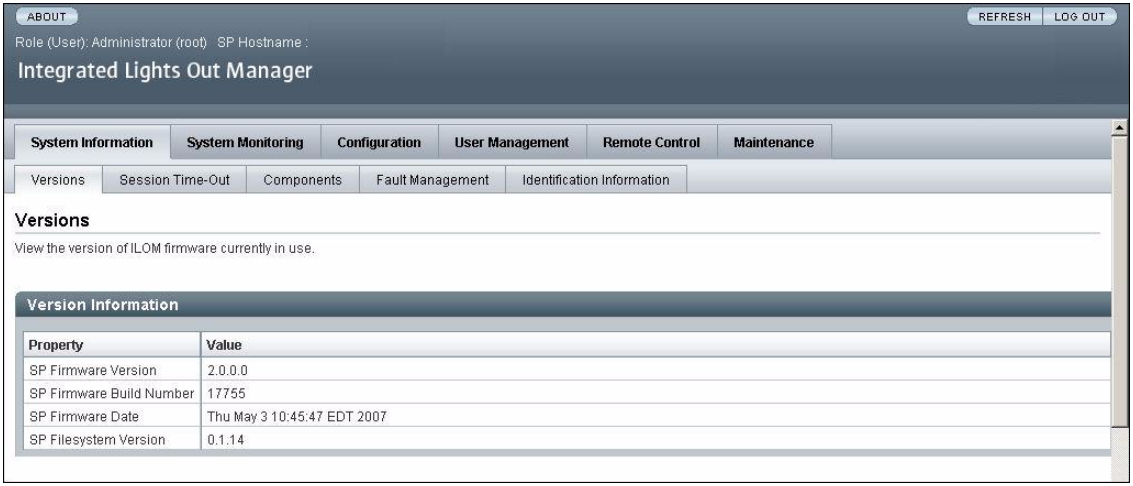
Standardbenutzername und Standardpasswort bestehen aus Kleinbuchstaben.

Für den Benutzernamen `root`, dem die Administrator-Rolle zugewiesen ist, ist eine lokale Benutzer-ID-Nummer vordefiniert. Diese Benutzer-ID-Nummer kann nicht gelöscht oder deren Rollenattribute geändert werden. Das anfängliche Passwort `changeme` wird ebenfalls bereitgestellt. Dieses Passwort ist zum Anmelden bei der CLI (Command-Line Interface, Befehlszeilenschnittstelle), der Secure Shell (SSH) und der Webbenutzeroberfläche erforderlich.

3. **Klicken Sie auf Log In.**

   Die Webbenutzeroberflächenseite Versions wird angezeigt.

**ABBILDUNG 4-9** Seite Versions




Nachdem Sie sich bei ILOM angemeldet und eine Netzwerkverbindung mit dem System hergestellt haben, müssen Sie das Passwort (`changeme`), das dem root-Konto von ILOM zugeordnet ist, ändern, um das System vor nicht autorisierten Zugriffen zu schützen. Informationen zum Ändern des Passworts des root-Kontos von ILOM finden Sie unter „Ändern des Passworts des root-Kontos in ILOM mithilfe der Webbenutzeroberfläche“ auf Seite 66.

# ▼ Hochladen des SSL-Zertifikats

ILOM bietet ein SSL-Standardzertifikat sowie einen selbstsignierten Schlüssel für den HTTPS-Zugriff.

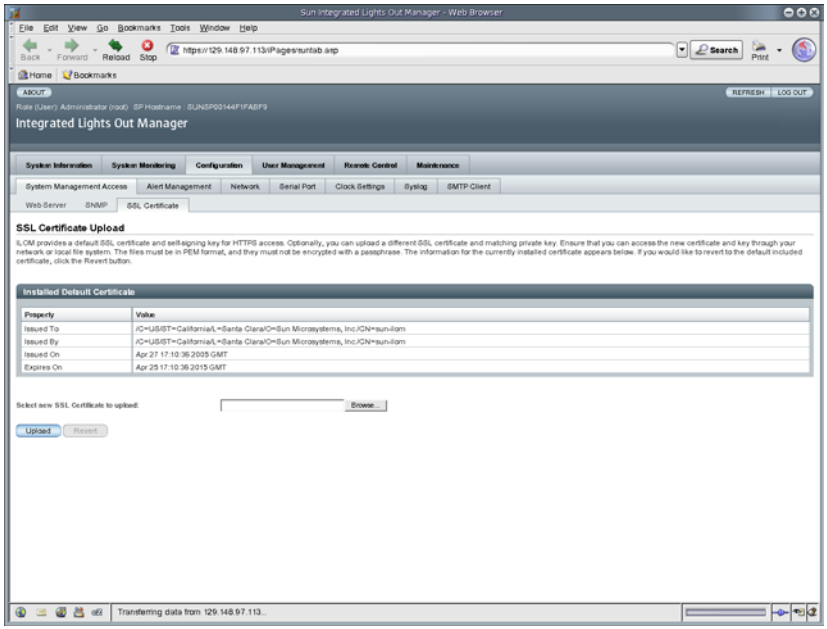
Optional können Sie ein anderes SSL-Zertifikat mit entsprechendem privatem Schlüssel hochladen. Stellen Sie sicher, dass Sie über Ihr Netzwerk oder lokales Dateisystem auf das neue Zertifikat und den Schlüssel zugreifen können.

Führen Sie diese Schritte durch, um das SSL-Zertifikat hochzuladen:

1. **Melden Sie sich bei ILOM an.**
2. **Wählen Sie Configuration --> System Management Access --> SSL Certificate.**

   Die Seite SSL Certificate Upgrade wird angezeigt.

**ABBILDUNG 4-10** Seite SSL Certificate Upload




3. **Geben Sie den Dateinamen des neuen SSL-Zertifikats ein, oder klicken Sie auf die Schaltfläche Browse, um nach einem neuen SSL-Zertifikat zu suchen.**

   Der Dateiname hat eine .pem-Dateierweiterung. Der Service-Prozessor unterstützt keine mit Passphrasen verschlüsselten Zertifikate.

4. **Klicken Sie auf die Schaltfläche Upload, um das ausgewählte SSL-Zertifikats abzurufen.**

   Das Dialogfeld SSL Certificate Upload Status wird angezeigt.

5. **Nachdem das Zertifikat und der private Schlüssel hochgeladen sind, klicken Sie auf die Schaltfläche OK, um den ILOM-Webserver zurückzusetzen, damit er nun das neue SSL-Zertifikat verwendet.**

   Der ILOM-Webserver muss zurückgesetzt werden, damit das neue Zertifikat übernommen wird.

## ▼ Festlegen der Sitzungszeitüberschreitung

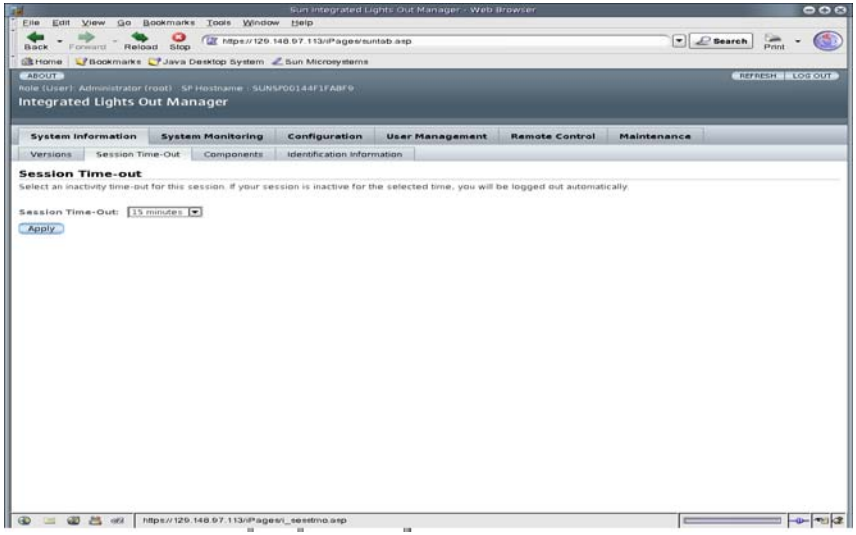
Die Einstellung der Sitzungszeitüberschreitung hat nur für die aktuelle ILOM-Sitzung Gültigkeit und bleibt nicht über das Abmelden hinaus erhalten. Die Sitzungszeitüberschreitung muss bei jeder Anmeldung bei der ILOM-Webbenutzeroberfläche neu festgelegt werden.

Führen Sie diese Schritte durch, um den Zeitraum festzulegen, über den eine ILOM-Sitzung im Leerlauf bleiben darf, bevor eine Abmeldung erfolgt:

1. **Melden Sie sich bei ILOM an.**
2. **Wählen Sie System Information -> Session Time-Out.**

   Die Seite Session Time-Out wird angezeigt.

**ABBILDUNG 4-11** Registerkarte Session Time-Out




3. **Wählen Sie im Dropdown-Listenfeld Session Time-Out den Zeitraum aus, über den die ILOM-Sitzung ohne ILOM-Aktivität im Leerlauf bleiben darf.**

   Sobald die Sitzung über den gewählten Zeitraum inaktiv gewesen ist, werden Sie automatisch von ILOM abgemeldet.

## ▼ Abmelden von ILOM

- **Klicken Sie zum Abmelden von der Webbenutzeroberfläche auf die Schaltfläche Log Out.**

  Die Schaltfläche Log Out befindet sich in der oberen rechten Ecke der Webbenutzeroberfläche.

KAPITEL 5

# Verwalten von Benutzerkonten

ILOM unterstützt bis zu 10 Benutzerkonten. Eines dieser Konten ist das vorkonfigurierte Administratorkonto, das Lese- und Schreibzugriff auf alle ILOM-Leistungsmerkmale, -Funktionen und -Befehle gewährt. Mithilfe der ILOM-Webbenutzeroberfläche oder der Befehlszeilenschnittstelle (CLI) können Benutzerkonten hinzugefügt, geändert und gelöscht werden.

Dieses Kapitel enthält folgende Abschnitte:


- „Richtlinien für die Verwaltung von Benutzerkonten“ auf Seite 65
- „Benutzerkontenrollen und -berechtigungen“ auf Seite 65
- „Vorkonfigurierte ILOM-Administratorkonten“ auf Seite 66
  - „Ändern des Passworts des root-Kontos in ILOM mithilfe der Webbenutzeroberfläche“ auf Seite 66
  - „Ändern des Passworts des root-Kontos in ILOM mithilfe der CLI“ auf Seite 69
- „Single Sign On“ auf Seite 69
  - „Aktivieren und Deaktivieren von Single Sign On mithilfe der CLI“ auf Seite 69
  - „Aktivieren und Deaktivieren von Single Sign On mithilfe der Webbenutzeroberfläche“ auf Seite 70
- „Verwalten von Benutzerkonten mithilfe der CLI“ auf Seite 70
  - „Hinzufügen eines Benutzerkontos mithilfe der CLI“ auf Seite 71
  - „Ändern eines Benutzerkontos mithilfe der CLI“ auf Seite 71
  - „Löschen eines Benutzerkontos mithilfe der CLI“ auf Seite 71
  - „Anzeigen einer Liste von Benutzerkonten mithilfe der CLI“ auf Seite 71
  - „Anzeigen eines einzelnen Benutzerkontos mithilfe der CLI“ auf Seite 72
  - „Konfigurieren eines Benutzerkontos mithilfe der CLI“ auf Seite 72
  - „Anzeigen einer Liste von Benutzersitzungen mithilfe der CLI“ auf Seite 73
  - „Anzeigen einer einzelnen Benutzersitzung mithilfe der CLI“ auf Seite 74
- „Verwalten von Benutzerkonten mithilfe der Webbenutzeroberfläche“ auf Seite 74

    - „Hinzufügen von Benutzerkonten und Festlegen von Berechtigungen mithilfe der Webbenutzeroberfläche“ auf Seite 74
    - „Ändern eines Benutzerkontos mithilfe der Webbenutzeroberfläche“ auf Seite 77
    - „Löschen eines Benutzerkontos mithilfe der Webbenutzeroberfläche“ auf Seite 80
    - „Anzeigen von Benutzersitzungen mithilfe der Webbenutzeroberfläche“ auf Seite 81
- „Active Directory“ auf Seite 82
    - „Konfigurieren von Active Directory mithilfe der Webbenutzeroberfläche“ auf Seite 83
    - „Bearbeiten von Active Directory-Tabelleninformationen mithilfe der Webbenutzeroberfläche“ auf Seite 88
    - „Ermitteln der Benutzerautorisierungsstufe“ auf Seite 89
    - „Absichern der Active Directory-Verbindung“ auf Seite 90
- „LDAP (Lightweight Directory Access Protocol)“ auf Seite 94
    - „Konfigurieren des LDAP-Servers“ auf Seite 97
    - „Konfigurieren von ILOM für LDAP mithilfe der CLI“ auf Seite 98
    - „Konfigurieren von ILOM für LDAP mithilfe der Webbenutzeroberfläche“ auf Seite 99
- „RADIUS-Authentifizierung“ auf Seite 100
    - „RADIUS-Clients und -Server“ auf Seite 100
    - „RADIUS-Parameter“ auf Seite 101
    - „Konfigurieren von RADIUS mithilfe der CLI“ auf Seite 102
    - „Konfigurieren von RADIUS mithilfe der Webbenutzeroberfläche“ auf Seite 102
    - „RADIUS-Befehle“ auf Seite 103


---

**Hinweis –** In diesem Kapitel verwendete Syntaxbeispiele verwenden das Ziel beginnend mit `/SP/`. Dies könnte in Abhängigkeit von der verwendeten Serverplattform gegen das Ziel beginnend mit `/CMM/` ausgetauscht werden. Unterziele sind auf allen Serverplattformen gleich.

---

# Richtlinien für die Verwaltung von Benutzerkonten

Berücksichtigen Sie die folgenden allgemeinen Richtlinien beim Verwalten von Benutzerkonten:

- ILOM unterstützt maximal 10 Benutzerkonten, von denen eines das vorkonfigurierte Administratorkonto ist. Das vorkonfigurierte Administratorkonto kann nicht gelöscht werden. Wenn alle zehn Benutzerkonten konfiguriert sind, muss zuerst ein vorhandenes Benutzerkonto gelöscht werden, um ein neues Benutzerkonto hinzufügen zu können.
- Nur Konten mit Administratorberechtigungen dürfen Benutzerkonten hinzufügen, ändern und löschen. Ein Benutzer mit Operatorberechtigungen darf aber das eigene Passwort ändern.
- Der Benutzername eines Kontos muss mindestens vier und darf höchstens 16 Zeichen lang sein. Benutzernamen unterscheiden zwischen Groß- und Kleinschreibung und müssen mit einem Buchstaben beginnen. Verwendet werden können Buchstaben, Zahlen, Binde- und Unterstriche. Benutzernamen dürfen keine Leerzeichen enthalten.
- Sie können entweder lokale Konten konfigurieren oder ILOM Konten gegen eine entfernte Benutzerdatenbank wie Active Directory, LDAP oder RADIUS authentifizieren lassen. Bei der entfernten Authentifizierung bietet es sich eher an, eine zentralisierte Benutzerdatenbank zu verwenden, anstatt lokale Konten auf jeder ILOM-Instanz zu konfigurieren. Darüber hinaus reicht es bei der entfernten Authentifizierung aus, das Passwort eines Benutzers einmal auf dem Server zu ändern.

# Benutzerkontenrollen und -berechtigungen

Benutzerkonten verfügen über zwei definierte Rollen. Jede Rolle gewährt ILOM-Benutzern bestimmte Berechtigungen. Zu den Benutzerrollen und -berechtigungen gehören:

- **Administrator** – Ermöglicht den Zugriff auf alle ILOM-Leistungsmerkmale, -Funktionen und -Befehle.
- **Operator** – Ermöglicht eingeschränkten Zugriff auf ILOM-Leistungsmerkmale, -Funktionen und -Befehle. Im Allgemeinen dürfen Operatoren keine Konfigurationseinstellungen ändern.

# Vorkonfigurierte ILOM-Administratorkonten

Zu den vorkonfigurierten ILOM-Administratorkonten, auch bekannt als „feste Benutzerkonten“, gehören:

**Benutzername**: `root`

**Passwort**: `changeme`

Der Benutzername `root` kann weder gelöscht noch geändert werden. Das Passwort (`changeme`) kann dagegen geändert werden. Dieses Konto bietet integrierte Administratorberechtigungen (Lese- und Schreibzugriff) für alle ILOM-Leistungsmerkmale, -Funktionen und -Befehle.

Beim ersten Zugriff auf ILOM auf SP- oder CMM-Ebene müssen Sie sich als `root` mit dem Standardpasswort `changeme` anmelden. Nachdem Sie sich bei ILOM angemeldet und eine Netzwerkverbindung mit dem System hergestellt haben, müssen Sie das Passwort (`changeme`), das dem `root`-Konto von ILOM zugeordnet ist, ändern, um das System vor nicht autorisierten Zugriffen zu schützen. Bei Verwendung eines Blade-Serversystems müssen Sie dieses Passwort auf jedem im Systemgehäuse installierten CMM und Blade ändern. Weitere Informationen zum Ändern des Passworts des `root`-Kontos in ILOM finden Sie unter „Ändern des Passworts des root-Kontos in ILOM mithilfe der Webbenutzeroberfläche“ auf Seite 66.

## ▼ Ändern des Passworts des root-Kontos in ILOM mithilfe der Webbenutzeroberfläche

Führen Sie diese Schritte durch, um das Passwort für das `root`-Konto zu ändern:

1. **Öffnen Sie einen Webbrowser, und geben Sie die IP-Adresse eines Server-SP oder CMM ein.**

   Die Anmeldeseite der ILOM-Webbenutzeroberfläche wird angezeigt.

2. **Führen Sie auf der Seite ILOM Login Folgendes aus:**

   a. **Geben Sie den Standardbenutzername (`root`) und das Standardpasswort (`changeme`) ein.**

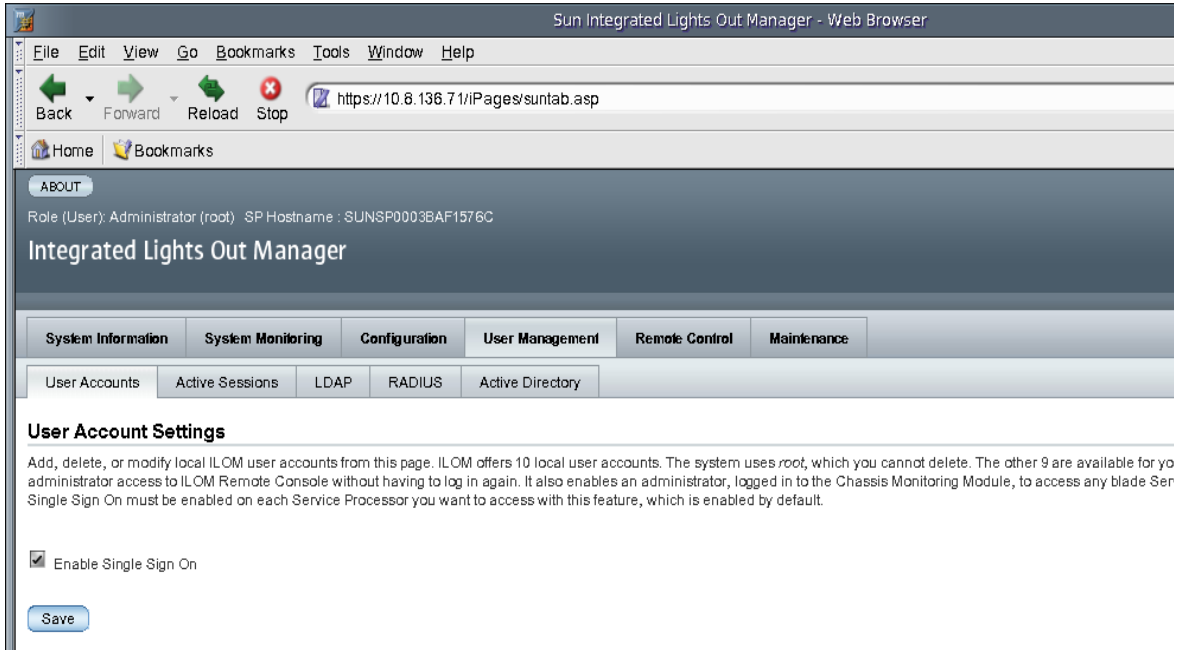
   b. **Klicken Sie auf Log In.**

      Die ILOM-Webbenutzeroberfläche wird angezeigt.

3. **Führen Sie in der ILOM-Webbenutzeroberfläche Folgendes aus:**
   - Klicken Sie zum Ändern des vorkonfigurierten Administratorpassworts auf das Gerät im linken Navigationsteilfenster, und fahren Sie dann mit Schritt 4 fort.
   - Klicken Sie zum Ändern des vorkonfigurierten Administratorpassworts auf der Blade-SP-Ebene auf das entsprechende Blade im linken Navigationsteilfenster, und fahren Sie dann mit Schritt 4 fort.
4. **Klicken Sie in der ILOM-Webbenutzeroberfläche auf User Management --> User Accounts.**

   Die Seite User Account Settings wird angezeigt.

**ABBILDUNG 5-1** Seite User Account Settings

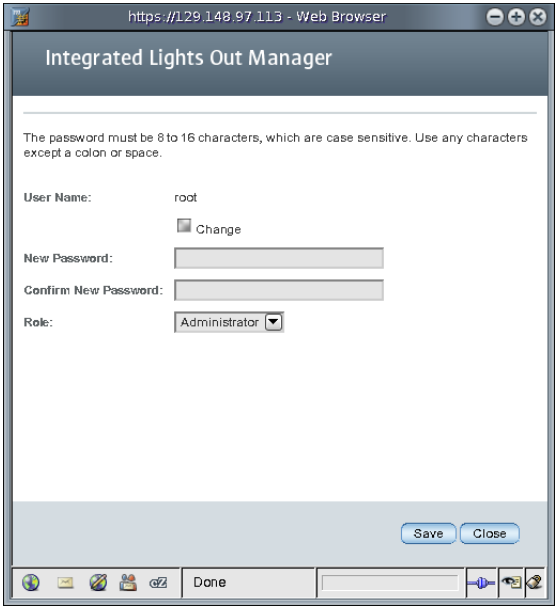

Sun Integrated Lights Out Manager - Web Browser
File Edit View Go Bookmarks Tools Window Help
Back Forward Reload Stop
https://10.8.136.71/iPages/suntab.asp
Home Bookmarks
ABOUT
Role (User): Administrator (root) SP Hostname : SUNSP0003BAF1576C
Integrated Lights Out Manager
System Information
System Monitoring
Configuration
User Management
Remote Control
Maintenance
User Accounts
Active Sessions
LDAP
RADIUS
Active Directory
User Account Settings
Add, delete, or modify local ILOM user accounts from this page. ILOM offers 10 local user accounts. The system uses root, which you cannot delete. The other 9 are available for yo
administrator access to ILOM Remote Console without having to log in again. It also enables an administrator, logged in to the Chassis Monitoring Module, to access any blade Ser
Single Sign On must be enabled on each Service Processor you want to access with this feature, which is enabled by default.
Enable Single Sign On
Save

5. **Aktivieren Sie auf der Seite User Account Settings das Optionsfeld neben `root`, und klicken Sie auf Edit.**

   Eine Sicherheitsmeldung wird angezeigt.

6. **Klicken Sie auf OK, um den Vorgang fortzusetzen. Das Dialogfeld User Account Password wird angezeigt.**

**ABBILDUNG 5-2** Dialogfeld User Account Password




7. **Führen Sie im Dialogfeld User Account Password Folgendes aus:**

   a. **Wählen Sie das Feld neben Change.**

   b. **Geben Sie in das Textfeld New Password das neue Passwort ein.**

   c. **Geben Sie in das Textfeld Confirm Password erneut das neue Passwort ein.**

   d. **Klicken Sie auf Save.**

      Das in den Schritten 6b und 6c angegebene neue Passwort ist für das Administratorkonto `root` aktiviert.

8. **Wiederholen Sie nötigenfalls die Schritte 2 bis 6d, um das Passwort für jedes installierte Gerät zu ändern.**

## ▼ Ändern des Passworts des root-Kontos in ILOM mithilfe der CLI

- **Geben Sie folgenden Befehl ein, um das Passwort des root-Kontos in ILOM zu ändern:**

```
-> set /SP/users/root password=passwort
```

Beispiel:

```
-> set /SP/users/root password=Passwort
Changing password for user /SP/users/root...
Enter new password again: ********
New password was successfully set for user /SP/users/root
```

# Single Sign On

Single Sign On (Einmalanmeldung) ist ein bequemer Authentifizierungsdienst, mit dem die Anzahl der erforderlichen Passworteingaben, um Zugriff auf ILOM zu erlangen, reduziert wird. Single Sign On ist standardmäßig aktiviert. Wie bei jedem anderen Authentifizierungsdienst auch, werden hierbei Authentifizierungsberechtigungsnachweise über das Netzwerk übermittelt. Wenn dies nicht gewünscht wird, muss der Single Sign On-Authentifizierungsdienst deaktiviert werden.

## ▼ Aktivieren und Deaktivieren von Single Sign On mithilfe der CLI

Single Sign On ist standardmäßig aktiviert. Nur Administratoren können Single Sign On deaktivieren bzw. aktivieren.

- **Geben Sie folgenden Befehl ein, um Single Sign On zu aktivieren oder zu deaktivieren:**

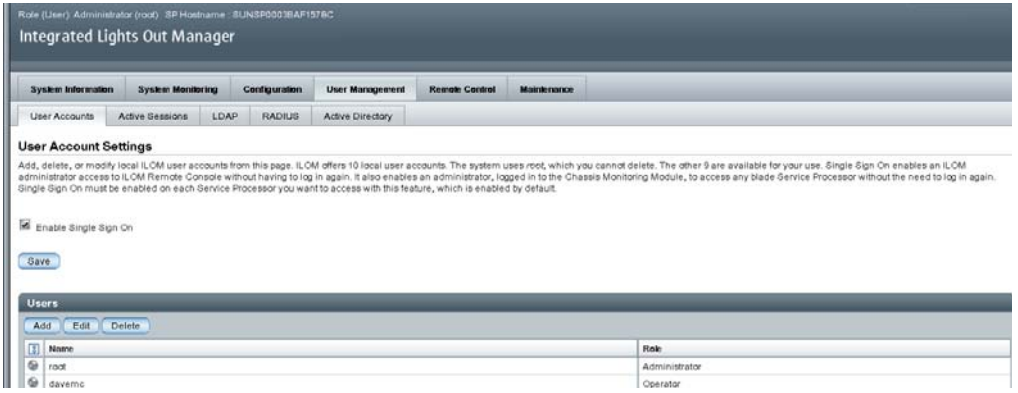
```
–> set /SP/services/sso state=disabled|enabled
```

## ▼ Aktivieren und Deaktivieren von Single Sign On mithilfe der Webbenutzeroberfläche

Führen Sie diese Schritte durch, um Single Sign On zu aktivieren bzw. deaktivieren:

1. **Melden Sie sich bei der ILOM-Webbenutzeroberfläche als Administrator an.**
2. **Wählen Sie User Management --> User Accounts.**
   Die Seite User Account Settings wird angezeigt.
3. **Klicken Sie auf das Kontrollkästchen neben Enable Single Sign On, um die Funktion zu aktivieren, oder deaktivieren Sie das Kontrollkästchen, um die Funktion zu deaktivieren.**

**ABBILDUNG 5-3** Seite User Account Settings mit aktiviertem Single Sign On




# Verwalten von Benutzerkonten mithilfe der CLI

In diesem Abschnitt wird beschrieben, wie Benutzerkonten mithilfe der ILOM-CLI verwaltet werden.

## ▼ Hinzufügen eines Benutzerkontos mithilfe der CLI

- **Geben Sie folgenden Befehl ein, um ein lokales Benutzerkonto hinzuzufügen:**

**–> create /SP/users/***Benutzername* **password=***Passwort* **role=**
**administrator|operator**

Beispiel:

```
-> create /SP/users/davemc
Creating user...
Enter new password: ********
Enter new password again: ********
Created /SP/users/davemc
```

## ▼ Ändern eines Benutzerkontos mithilfe der CLI

- **Geben Sie folgenden Befehl ein, um ein lokales Benutzerkonto zu ändern:**

**–> set /SP/users/***Benutzername* **password=***Passwort* **role=**
**administrator|operator**

## ▼ Löschen eines Benutzerkontos mithilfe der CLI

1. **Geben Sie folgenden Befehl ein, um ein lokales Benutzerkonto zu löschen:**

**–> delete /SP/users/***Benutzername*

Beispiel:

```
->delete /SP/users/davemc
  Are you sure you want to delete /SP/users/davemc (y/n)?
```

2. **Type `y` to delete, or `n` to cancel.**

## ▼ Anzeigen einer Liste von Benutzerkonten mithilfe der CLI

- **Geben Sie folgenden Befehl ein, um Informationen zu einem bestimmten lokalen Benutzerkonto anzuzeigen:**

**–> show -display targets /SP/users**

Beispiel:

```
-> show -display targets /SP/users
 /SP/users
    Targets:
        root
        davemc
```

## ▼ Anzeigen eines einzelnen Benutzerkontos mithilfe der CLI

- **Geben Sie folgenden Befehl ein, um Informationen zu einem bestimmten Benutzerkonto anzuzeigen:**

**–> show /SP/users/***Benutzername*

Beispiel:

```
-> show /SP/users/davemc
 /SP/users/davemc
    Targets:
    Properties:
        role = Operator
        password = *****
    Commands:
        cd
        set
        show
```

## ▼ Konfigurieren eines Benutzerkontos mithilfe der CLI

Mit dem Befehl `set` können Sie Ziele, Eigenschaften, Passwörter und Werte für konfigurierte Benutzerkonten ändern.

- **Geben Sie folgenden Befehl ein, um ein lokales Benutzerkonto zu konfigurieren:**

**–> set <***Ziel***> [<***Eigenschaft***>=***Wert***]**

## Ziele, Eigenschaften und Werte

Folgende Ziele, Eigenschaften und Werte sind für lokale Benutzerkonten gültig.

**TABELLE 5-1** Gültige Ziele, Eigenschaften und Werte für lokale Benutzerkonten

| Ziel | Eigenschaft | Wert | Passwort | Standard |
|---|---|---|---|---|
| /SP/users/*Benutzername* | role | administrator \| operator | | operator |
| | password | <Zeichenfolge> | | |

Geben Sie Folgendes ein, um beispielsweise die Rolle für `user1` von „administrator“ in „operator“ zu ändern:

```
–> set /SP/users/user1 role=operator
```

Geben Sie zum Ändern des Passworts für `user1` Folgendes ein:

```
–> set /SP/users/user1 password
Changing password for user /SP/users/user1/password...
Enter new password:********
Enter new password again:********
New password was successfully set for user /SP/users/user1
```

**Hinweis –** Zum Ändern von Benutzereigenschaften müssen Sie über Administratorberechtigungen verfügen.

# ▼ Anzeigen einer Liste von Benutzersitzungen mithilfe der CLI

- **Geben Sie folgenden Befehl ein, um Informationen zu allen lokalen Benutzersitzungen anzuzeigen:**

```
–> show /SP/sessions
```

Beispiel:

```
-> show /SP/sessions
 /SP/sessions
    Targets:
        108
    Properties:
    Commands:
        cd
        show
```

## ▼ Anzeigen einer einzelnen Benutzersitzung mithilfe der CLI

- **Geben Sie folgenden Befehl ein, um Informationen zu einer einzelnen Benutzersitzung anzuzeigen:**

**–> show /SP/sessions/108**

Beispiel:

```
-> show /SP/sessions/108
/SP/sessions/108
   Targets:
   Properties:
       username = root
       starttime = Tue Jun  5 10:04:05 2007
       type = shell
   Commands:
       cd
       show
```

# Verwalten von Benutzerkonten mithilfe der Webbenutzeroberfläche

In diesem Abschnitt wird beschrieben, wie Benutzerkonten mithilfe der Webbenutzeroberfläche hinzugefügt, geändert und gelöscht werden.

## ▼ Hinzufügen von Benutzerkonten und Festlegen von Berechtigungen mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich bei der ILOM-Webbenutzeroberfläche als Benutzer mit Administratorberechtigungen an.**

   Nur Konten mit Administratorberechtigungen dürfen Benutzerkonten hinzufügen, ändern und löschen. Operatoren können aber das eigene Passwort ändern.

   Wenn ein neuer Benutzer Administratorberechtigungen erhält, werden diese automatisch ebenfalls für die CLI und die IPMI (Intelligent Platform Management Interface) von ILOM gewährt.

2. **Wählen Sie User Management --> User Accounts.**

   Die Seite User Account Settings wird angezeigt.

3. **Klicken Sie in der Tabelle Users auf Add.**

   Das Dialogfeld Add User wird angezeigt.

**ABBILDUNG 5-4** Dialogfeld Add User

https://129.148.97.113 - Web Browser
Integrated Lights Out Manager
The user name must be 4 to 16 characters and must start with an alphabetic character and use no spaces. The password must be 8 to 16 characters, which are case sensitive. Use any characters except a colon or space.
User Name:
Password:
Confirm Password:
Role:
Operator
Save
Close
Done

4. **Ergänzen Sie die folgenden Informationen:**

   a. **Geben Sie einen Benutzernamen in das Feld User Name ein.**

   b. **Geben Sie ein Passwort in das Feld Password ein.**

      Das Passwort muss mindestens 8 Zeichen und darf höchstens 16 Zeichen lang sein. Das Passwort unterscheidet zwischen Groß- und Kleinschreibung. Verwenden Sie Buchstaben, Zahlen und Sonderzeichen, um die Sicherheit zu erhöhen. Es können beliebige Zeichen mit Ausnahme des Doppelpunkts verwendet werden. Passwörter dürfen keine Leerzeichen enthalten.

   c. **Geben Sie das Passwort im Feld Confirm Password erneut ein, um es zu bestätigen.**

   d. **Wählen Sie im Dropdown-Listenfeld Role den Eintrag Administrator oder Operator.**

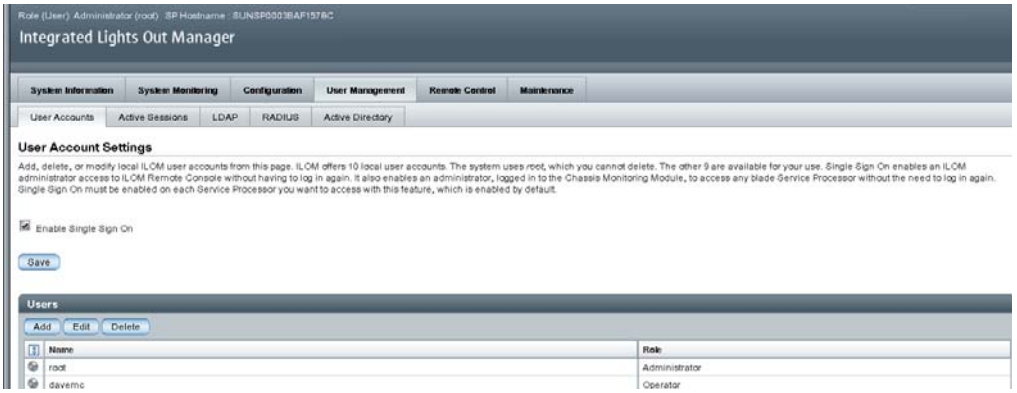
**ABBILDUNG 5-5** Dialogfeld Add User mit ausgefüllten Feldern

https://129.148.97.113 - Web Browser
Integrated Lights Out Manager
The user name must be 4 to 16 characters and must start with an alphabetic character and use no spaces. The password must be 8 to 16 characters, which are case sensitive. Use any characters except a colon or space.
User Name:
davemc
Password:
********
Confirm Password:
********
Role:
Administrator
Save
Close
Done

**e. Wenn Sie mit der Eingabe der Informationen für den neuen Benutzer fertig sind, klicken Sie auf Save.**

Die Seite User Account Settings wird erneut angezeigt. Das neue Benutzerkonto mit den zugeordneten Informationen wird nun auf der Seite User Account Settings aufgeführt.

**ABBILDUNG 5-6** Seite User Account Settings mit Anzeige des neuen Benutzers




# ▼ Ändern eines Benutzerkontos mithilfe der Webbenutzeroberfläche

In diesem Abschnitt wird beschrieben, wie ein ILOM-Benutzerkonto geändert wird. Das Ändern eines Benutzerkontos kann das Ändern des Passworts des Benutzers und der Netzwerk- und seriellen Berechtigungen umfassen.

---

**Hinweis –** Nur Konten mit Administratorberechtigungen dürfen Benutzerkonten hinzufügen, ändern und löschen. Operatoren können aber das eigene Passwort ändern.

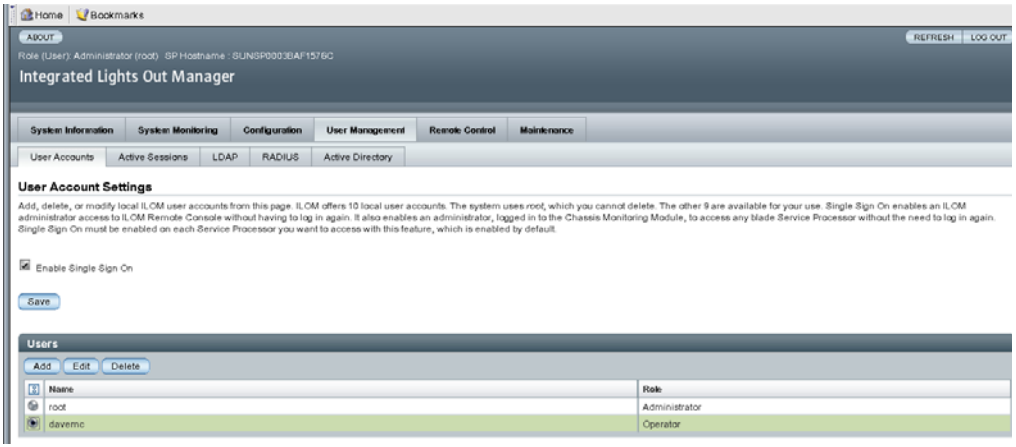
---

Wenn ein neuer Benutzer Administratorberechtigungen erhält, werden diese automatisch ebenfalls für die CLI und die IPMI (Intelligent Platform Management Interface) von ILOM gewährt.

1. **Melden Sie sich bei ILOM als Administrator an, um die Webbenutzeroberfläche zu öffnen.**
2. **Wählen Sie User Management --> User Accounts.**

   Die Seite User Account Settings wird angezeigt.

**ABBILDUNG 5-7** Seite User Account Settings

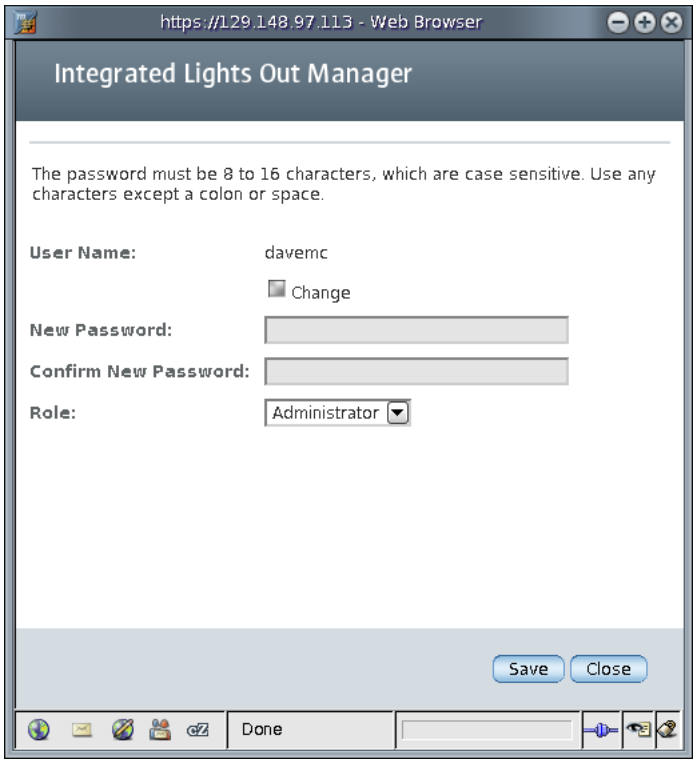

Home
Bookmarks
ABOUT
REFRESH
LOG OUT
Role (User): Administrator (root) SP Hostname : SUNSP0003BAF1576C
Integrated Lights Out Manager
System Information
System Monitoring
Configuration
User Management
Remote Control
Maintenance
User Accounts
Active Sessions
LDAP
RADIUS
Active Directory
User Account Settings
Add, delete, or modify local ILOM user accounts from this page. ILOM offers 10 local user accounts. The system uses root, which you cannot delete. The other 9 are available for your use. Single Sign On enables an ILOM administrator access to ILOM Remote Console without having to log in again. It also enables an administrator, logged in to the Chassis Monitoring Module, to access any blade Service Processor without the need to log in again. Single Sign On must be enabled on each Service Processor you want to access with this feature, which is enabled by default.
Enable Single Sign On
Save
Users
Add
Edit
Delete
Name
Role
root
Administrator
daveme
Operator

3. **Aktivieren Sie in der Tabelle Users das Optionsfeld neben dem Benutzerkonto, das geändert werden soll.**

4. **Klicken Sie auf Edit.**

   Das Dialogfeld Edit User wird angezeigt.

**ABBILDUNG 5-8** Dialogfeld Edit User




5. **Ändern Sie das Passwort, falls erforderlich.**

   a. **Aktivieren Sie das Kontrollkästchen Change, wenn das Benutzerpasswort geändert werden soll. Soll das Passwort nicht geändert werden, muss das Kontrollkästchen deaktiviert werden.**

   b. **Geben Sie ein neues Passwort in das Feld New Password ein.**

      Das Passwort muss zwischen 8 und 16 Zeichen lang sein. Das Passwort unterscheidet zwischen Groß- und Kleinschreibung. Verwenden Sie Buchstaben, Zahlen und Sonderzeichen, um die Sicherheit zu erhöhen. Es können beliebige Zeichen mit Ausnahme des Doppelpunkts verwendet werden. Passwörter dürfen keine Leerzeichen enthalten.

   c. **Geben Sie das Passwort im Feld Confirm New Password erneut ein, um es zu bestätigen.**

6. **Wählen Sie im Dropdown-Listenfeld Role den Eintrag Administrator oder Operator.**

7. **Klicken Sie nach dem Ändern der Kontoinformationen auf Save, um die Änderungen zu übernehmen, oder auf Close, um zu den vorherigen Einstellungen zurückzukehren.**

   Die Seite User Account Settings wird erneut angezeigt.

## ▼ Löschen eines Benutzerkontos mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich bei ILOM als Administrator an, um die Webbenutzeroberfläche zu öffnen.**
2. **Wählen Sie User Management --> User Accounts.**

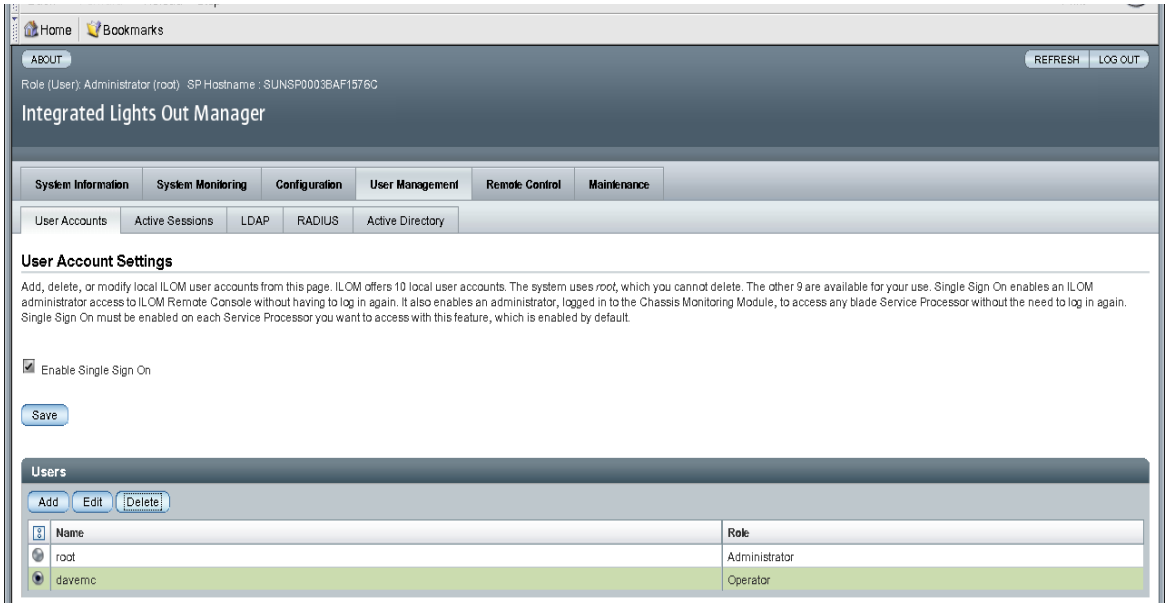
   Die Seite User Account Settings wird angezeigt.
3. **Aktivieren Sie das Optionsfeld neben dem Benutzerkonto, das gelöscht werden soll.**

---

**Hinweis –** Das root-Konto kann nicht gelöscht werden.

---

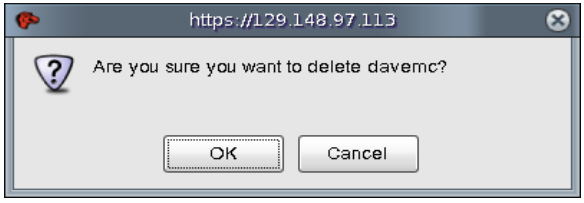
**ABBILDUNG 5-9** Seite User Account Settings


Home
Bookmarks
ABOUT
REFRESH
LOG OUT
Role (User): Administrator (root) SP Hostname : SUNSP0003BAF1576C
Integrated Lights Out Manager
System Information
System Monitoring
Configuration
User Management
Remote Control
Maintenance
User Accounts
Active Sessions
LDAP
RADIUS
Active Directory
User Account Settings
Add, delete, or modify local ILOM user accounts from this page. ILOM offers 10 local user accounts. The system uses root, which you cannot delete. The other 9 are available for your use. Single Sign On enables an ILOM administrator access to ILOM Remote Console without having to log in again. It also enables an administrator, logged in to the Chassis Monitoring Module, to access any blade Service Processor without the need to log in again. Single Sign On must be enabled on each Service Processor you want to access with this feature, which is enabled by default.
Enable Single Sign On
Save
Users
Add
Edit
Delete
Name
Role
root
Administrator
davemc
Operator

4. **Klicken Sie in der Tabelle Users auf Delete.**

   Das Bestätigungsdialogfeld wird angezeigt.

**ABBILDUNG 5-10** Bestätigungsdialogfeld zum Löschen eines Benutzers




5. **Klicken Sie auf OK, um das Konto zu löschen, oder auf Cancel, um den Prozess zu beenden.**

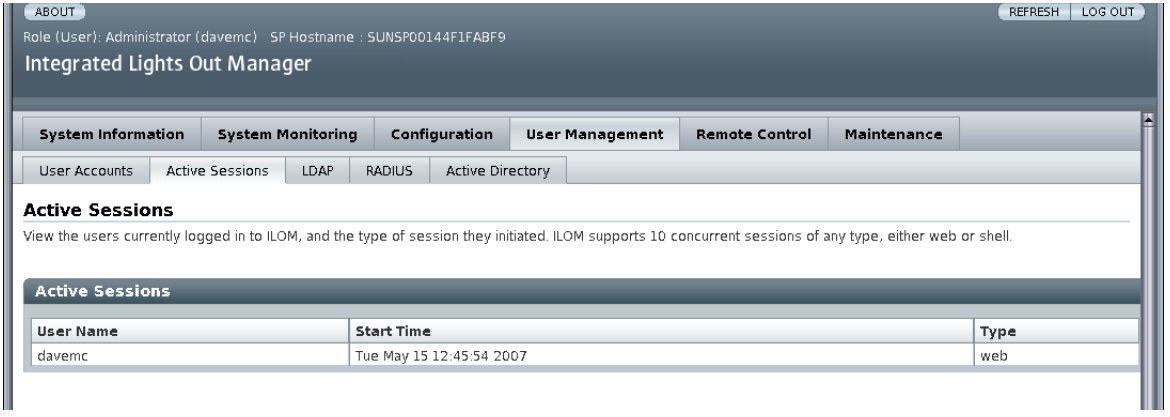
   Die Seite User Account Settings wird nun ohne das gelöschte Benutzerkonto angezeigt.

## ▼ Anzeigen von Benutzersitzungen mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich bei der ILOM-Webbenutzeroberfläche an.**
2. **Wählen Sie User Management --> Active Sessions.**

   Die Seite Active Sessions wird angezeigt. Angezeigt werden der Benutzername, Datum und Uhrzeit des Sitzungsbeginns sowie die Typen von Sitzungen der aktuell bei ILOM angemeldeten Benutzer.

**ABBILDUNG 5-11** Seite Active Sessions



# Active Directory

ILOM unterstützt Active Directory, den verteilten Verzeichnisdienst der Betriebssysteme Microsoft Windows Server 2003 und Microsoft Windows 2000 Server.

## Informationen zu Active Directory

Ein Verzeichnisdienst ist sowohl ein Datenbankspeichersystem (Verzeichnisspeicher) als auch eine Gruppe von Diensten, die Funktionen zum sicheren Hinzufügen, Ändern, Löschen und Auffinden von Daten im Verzeichnisspeicher bereitstellen. In einer verteilten Umgebung stellt ein Verzeichnisdienst einen zentralen Ort zum Speichern von Informationen zu Netzwerkgeräten und -diensten sowie deren Benutzern bereit. Ein Verzeichnisdienst implementiert darüber hinaus die Dienste, mit deren Hilfe diese Informationen Benutzern, Computern und Anwendungen zur Verfügung gestellt werden.

Active Directory wird üblicherweise für einen der folgenden drei Zwecke eingesetzt:

- **Internes Verzeichnis** – Interne Verzeichnisse werden innerhalb des Unternehmensnetzwerks zum Veröffentlichen von Informationen zu Benutzern und Ressourcen innerhalb des Unternehmens verwendet.
- **Externes Verzeichnis** – Solche Verzeichnisse befinden sich normalerweise auf Servern im Netzwerk zur Außenwelt (Perimeter) oder in der DMZ (Demilitarized Zone) an der Grenze zwischen dem Unternehmens-LAN und dem öffentlichen Internet.
- **Anwendungsverzeichnis** – Anwendungsverzeichnisse speichern „private“ Verzeichnisdaten, die nur für die Anwendung relevant sind, in einem lokalen Verzeichnis, das sich möglicherweise auf demselben Server wie die Anwendung befindet, ohne dass eine zusätzliche Konfiguration von Active Directory erforderlich wäre.

Active Directory kann zum Authentifizieren von Benutzerberechtigungsnachweisen verwendet werden. Zugriffsstufen können konfiguriert oder auf Grundlage der Gruppenmitgliedschaft vom Server übernommen werden. Es kann mehr als eine Benutzerdomäne verwendet werden, und die konfigurierten Domänen werden in der Reihenfolge der Konfiguration abgefragt.

# Konfigurieren von Active Directory

Zum Konfigurieren von Active Directory müssen einige globale Eigenschaften festgelegt und Informationen in drei Tabellen angegeben werden, die Folgendes darstellen:

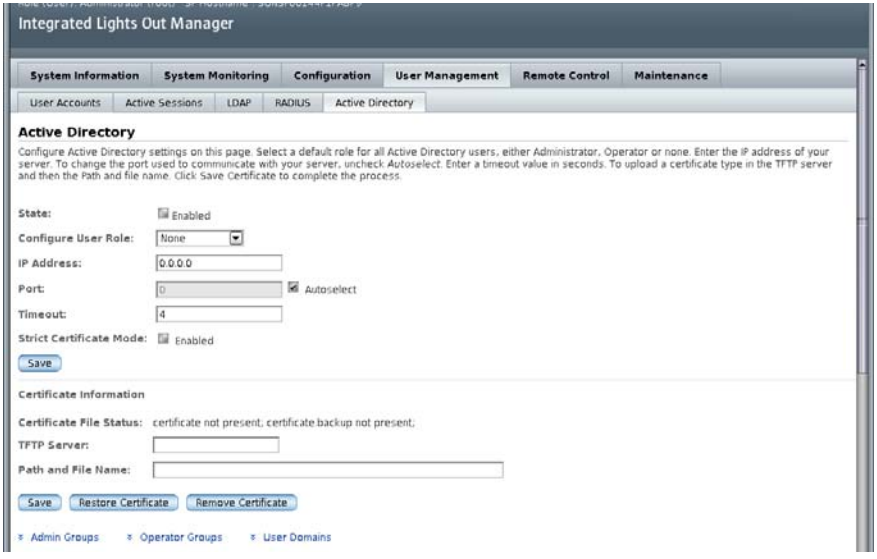
- Benutzerdomäne
- Administrator-Gruppen
- Operator-Gruppen

## ▼ Konfigurieren von Active Directory mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich bei ILOM als Benutzer mit Administratorberechtigungen an, um die Webbenutzeroberfläche zu öffnen.**
2. **Wählen Sie User Management --> Active Directory.**

   Die Seite Active Directory wird angezeigt. Die Active Directory-Konfigurationseinstellungen und Active Directory-Tabellen befinden sich auf dieser Seite in der oberen Hälfte.

**ABBILDUNG 5-12** Active Directory-Konfigurationseinstellungen



## Eigenschaften der Seite Active Directory-Konfiguration

In TABELLE 5-2 werden die Einstellungen beschrieben, die für die Verwendung von Active Directory konfiguriert werden müssen.

**TABELLE 5-2** Active Directory-Konfigurationseinstellungen (Globale Variablen)

| Eigenschaft (Web) | Eigenschaft (CLI) | Standard | Beschreibung |
|---|---|---|---|
| State | `adminState` | Enabled | Enabled \| Disabled |
| Role | `defaultRole` | None | None \| Administrator \| Operator<br>Im einfachen Konfigurationsszenario wird allen authentifizierten Benutzern die Zugriffsrolle gewährt. Standardmäßig ist diese Zugriffsrolle nicht konfiguriert, sodass der stärker integrierte Ansatz als Standardeinstellung aktiviert ist. Die Zugriffsstufe wird vom Active Directory-Server abgerufen. |
| IP Address | `ipaddress` | | IP-Adresse des Active Directory-Servers. |
| Port | `port` | 0 (autoselect) | Der für die Kommunikation mit dem Server verwendete Anschluss. Alternativ ist die Eingabe von „autoselect“ (automatische Auswahl) möglich.<br>Zeigt die Verwendung des Standardanschlusses für SSL-LDAP-Transaktionen an.<br>Im unwahrscheinlichen Fall verfügbar, dass ein nicht standardmäßiger TCP-Anschluss verwendet wird. |
| Timeout | `timeout` | 5 | Wert für Zeitüberschreitung in Sekunden.<br>Anzahl der Sekunden, die einzelnen LDAP-Transaktionen für deren Abschluss gewährt wird. Der Wert repräsentiert nicht die Gesamtzeit aller Transaktionen, weil die Anzahl der Transaktionen in Abhängigkeit von der Konfiguration schwanken kann.<br>Diese Eigenschaft ermöglicht das Einstellen der Wartezeit, wenn ein Server nicht antwortet oder nicht erreichbar ist. |

**TABELLE 5-2** Active Directory-Konfigurationseinstellungen (Globale Variablen) *(Fortsetzung)*

| Eigenschaft (Web) | Eigenschaft (CLI) | Standard | Beschreibung |
|---|---|---|---|
| Strict Certificate Mode | `strictcertmode` | Enabled | Enabled \| Disabled<br>Bei Aktivierung muss das Serverzertifikat hochgeladen sein, um eine restriktivere Zertifikatüberprüfung vorzunehmen. |
| Certificate File Status | `certfilestatus` | | certificate present \| not present; certificate.backup present \| not present |
| Keine entsprechende Webeigenschaft | `getcertfile` | nicht vorhanden | Methode zum Hochladen einer Zertifikatdatei, falls notwendig. Ein Zertifikat kann von hier aus auch entfernt oder wiederhergestellt werden. |
| TFTP Server | Keine entsprechende CLI-Eigenschaft | nicht vorhanden | Der zum Abrufen der Zertifikatdatei verwendete TFTP-Server. |
| Path and File Name | Keine entsprechende CLI-Eigenschaft | nicht vorhanden | Der vollständige Pfad- und Dateiname der Zertifikatdatei auf dem Server. |
| Restore Certificate | Keine entsprechende CLI-Eigenschaft | nicht vorhanden | Findet Verwendung, wenn eine Zertifikatdatei über eine vorhandene Zertifikatdatei hochgeladen wurde. Die vorhandene Datei wird als Sicherungskopie gespeichert. Durch die Wiederherstellung wird die Sicherungskopie wieder zum aktuellen Exemplar gemacht. |
| Remove Certificate | Keine entsprechende CLI-Eigenschaft | nicht vorhanden | Bei aktiviertem Strict Certificate Mode kann ein Zertifikat nicht entfernt werden. |

## Active Directory-Zieltabellen

Die drei Tabellen in der unteren Hälfte der Active Directory-Benutzeroberfläche (ABBILDUNG 5-13) werden zum Konfigurieren von Domänen und Gruppen verwendet, um Benutzer zu authentifizieren und zu autorisieren. In Zieltabellen werden Informationen zu folgenden Elementen gespeichert:

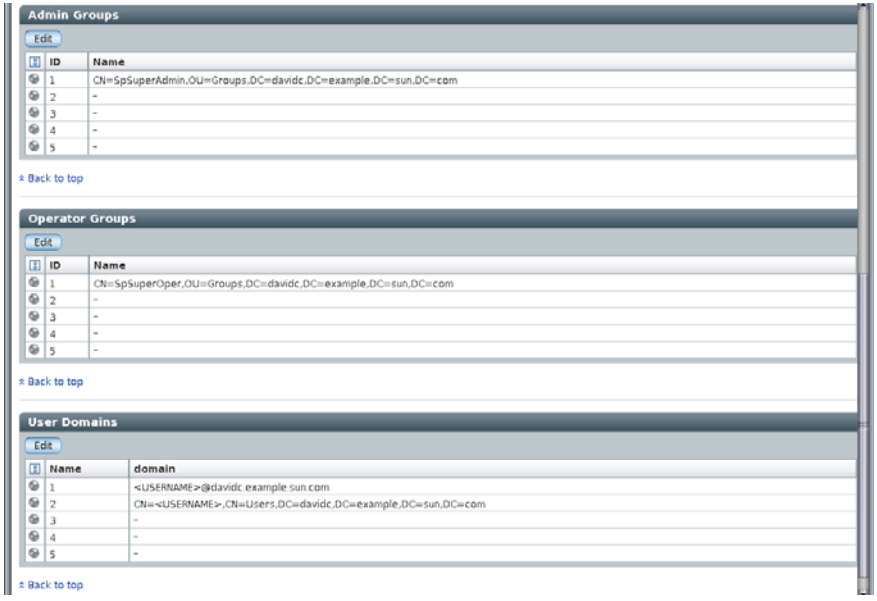
- Administrator-Gruppen
- Operator-Gruppen
- Benutzerdomänen

Tabelleneinträge zu Administrator- und Operator-Gruppen enthalten die Namen der MS Active Directory-Gruppen im Distinguished Name-Format (DN). Wenn ein Benutzer Mitglied einer bestimmten Gruppe ist, erhält dieser in Abhängigkeit von der Übereinstimmung zwischen Benutzergruppen und Tabellen Zugriff als Operator oder als Administrator.

Benutzerdomänen sind die Authentifizierungsdomänen, zu denen der Benutzer gehört. Üblicherweise wird der bei der Anmeldung eines Benutzers verwendete Name in dem spezifischen Domäne/Name-Format formatiert, das von diesen Einträgen bereitgestellt wird. Der Versuch einer Benutzerauthentifizierung erfolgt auf Grundlage der vom Benutzer eingegebenen Benutzerdomänendaten und des angegebenen Anmeldenamens.

Für alle drei Tabellen werden einige Standarddaten angegeben, um das erwartete Format der Daten zu veranschaulichen. In den Fehlermeldungen wird außerdem erläutert, was vom Benutzer eingegeben werden sollte.

**ABBILDUNG 5-13** Active Directory-Tabellen



## Eigenschaften von Active Directory-Zieltabellen

TABELLE 5-3 und TABELLE 5-4 bieten eine detailliertere Darstellung der Tabellen „Admin Groups“ und „Operator Groups“. In der Spalte Name werden vollständig qualifizierte DNs (Distinguished Name) angegeben.

**TABELLE 5-3** Tabelle Admin Groups

| ID | Name |
|---|---|
| 1 | CN=SpSuperAdmin,OU=Groups,DC=davidc,DC=example,DC=sun,DC=com |
| 2 | |

**TABELLE 5-4** Tabelle Operator Groups

| ID | Name |
|---|---|
| 1 | CN=SpSuperOper,OU=Groups,DC=davidc,DC=example,DC=sun,DC=com |
| 2 | |
| 3 | |
| 4 | |
| 5 | |

TABELLE 5-5 bietet eine detailliertere Darstellung der in ABBILDUNG 5-13 gezeigten Tabelle „User Domains“. Die in Eintrag 1 aufgeführte Domäne zeigt das Basisformat, das beim ersten Authentifizierungsversuch verwendet wird. Eintrag 2 zeigt den vollständigen Distinguished Name (`dn`), der verwendet wird, wenn der Authentifizierungsversuch mit dem Basisformat fehlschlägt.

**Hinweis –** In dem in TABELLE 5-5 verwendeten Beispiel stellt <BENUTZERNAME> die Platzhalterzeichenfolge dar, die durch den tatsächlichen Anmeldenamen eines Benutzers ersetzt wird.

**TABELLE 5-5** Tabelle User Domains

| Name | Domäne |
|---|---|
| 1 | `<BENUTZERNAME>@davidc.example.sun.com` |
| 2 | `CN=<BENUTZERNAME>,CN=Users,DC=davidc,DC=example,DC=sun,DC=com` |
| 3 | |
| 4 | |
| 5 | |

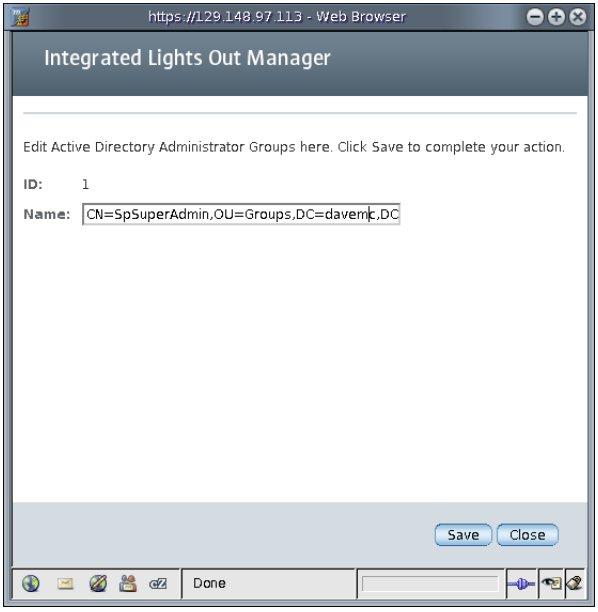
## ▼ Bearbeiten von Active Directory-Tabelleninformationen mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich bei ILOM als Benutzer mit Administratorberechtigungen an, um die Webbenutzeroberfläche zu öffnen.**
2. **Wählen Sie User Management --> Active Directory.**

   Die Seite Active Directory wird angezeigt.
3. **Aktivieren Sie unten auf der Seite Active Directory das Optionsfeld der Informationszeile, die bearbeitet werden soll, und klicken Sie auf Edit.**

   Die entsprechende Seite wird angezeigt: Seite Edit Active Directory Administrator Groups, Seite Edit Active Directory Operator Groups oder Seite Edit Active Directory User Domains. Auf jeder Bearbeitungsseite findet sich ein Feld Name zum Hinzufügen oder Bearbeiten von Informationen.

**ABBILDUNG 5-14** Seite zum Bearbeiten von Active Directory-Administratorgruppen




4. **Fügen Sie auf der Seite Edit die Informationen hinzu, oder bearbeiten Sie diese.**
5. **Klicken Sie auf Save, um die Änderungen zu übernehmen.**

   Die Seite Active Directory wird angezeigt.

6. **Geben Sie in der Tabelle User Domains die Informationen in das Feld Name als Text ein. Verwenden Sie den Platzhalter** `<BENUTZERNAME>`**, um Platz für den Namen des Benutzers in LDAP-Anforderungen freizuhalten.**

   Beispiel:

   ```
   domain = <BENUTZERNAME>@davemc.example.sun.com
   ```

   ```
   domain = CN=<BENUTZERNAME>,CN=Users,DC=davemc,DC=example,DC=
   sun,DC=com
   ```

   Bei Angabe beider in den folgenden Beispielen gezeigten Namen wird dem Benutzer Zugriff auf ILOM erteilt.

**CODE-BEISPIEL 5-1** Active Directory-Anmeldung mit dem Basisformat

```
/home/dc150698> ssh -l davemc 10.x.xxx.xxx
  Password:*******
  Sun(TM) Integrated Lights Out Manager
  Version 1.1
  Copyright 2005 Sun Microsystems, Inc. All rights reserved.
  ->
```

**CODE-BEISPIEL 5-2** Active Directory-Anmeldung mit dem Distinguished Name (DN)

```
/home/dc150698> ssh -l "David A. Engineer" 10.x.xxx.xxx
  Password:*******
  Sun(TM) Integrated Lights Out Manager
  Version 1.1
  Copyright 2005 Sun Microsystems, Inc. All rights reserved.
  ->
```

# Ermitteln der Benutzerautorisierungsstufe

Nach Abschluss der Authentifizierung kann die Zugriffsstufe des Benutzers auf folgende Weisen ermittelt werden. Im einfachsten Fall wird der Benutzerzugriff für den Typ „Operator“ oder „Administrator“ direkt aus der Konfiguration der Active Directory-Konfiguration des SP abgerufen. Eine stärker integrierte Vorgehensweise steht ebenfalls zur Verfügung, bei der eine Reihe von LDAP-Abfragen ausgeführt wird, um die Active Directory-Gruppen zu ermitteln, denen der Benutzer zugeordnet ist.

- Das erste Verfahren lässt sich am einfachsten konfigurieren. Hierbei ist der Benutzer immer noch mit der `defaultRole` authentifiziert, aber Abfragen zum Ermitteln der Gruppenmitgliedschaft sind nicht erforderlich. Das Einrichten von Benutzern in der Active Directory-Datenbank ist einfacher und erfordert unabhängig von der Gruppenmitgliedschaft nur ein Passwort. Auf dem SP wird die `defaultRole` entweder auf `administrator` oder auf `operator` festgelegt.

Allen über Active Directory authentifizierten Benutzern werden ausschließlich auf Grundlage dieser Konfiguration die Berechtigungen zugewiesen, die dem Administrator- oder Operator-Benutzer zugeordnet sind.

- Das zweite Verfahren gestaltet sich komplizierter und erfordert wesentlich mehr Aufwand bei der Konfiguration und Authentifizierung jedes einzelnen Benutzers. Für die Konfiguration müssen die SP-Tabellen Administrator Groups und Operator Groups mit den entsprechenden Gruppennamen aus der Active Directory-Datenbank konfiguriert sein, die zum Ermitteln der Zugriffsstufen verwendet werden. Bis zu fünf Active Directory-Gruppen können eingegeben werden, um einen Administrator zu bestimmen, und weitere fünf können für die Zuweisung von Operatorberechtigungen verwendet werden.

Die Gruppenmitgliedschaft des Benutzers wird zum Identifizieren der ordnungsgemäßen Zugriffsstufe „Administrator“ oder „Operator“ verwendet, indem jeder Gruppenname in den konfigurierten Active Directory-Tabellen auf dem SP nachgeschlagen wird. Bei Verwendung des zweiten Verfahrens werden fünf Benutzergruppen als mit Operatorberechtigungen ausgestattet identifiziert, und fünf Benutzergruppen werden als mit Administratorberechtigungen versehen identifiziert. Befindet sich die Liste der Gruppen des Benutzers in keiner der definierten SP-Benutzergruppen, wird der Zugriff verweigert.

## Absichern der Active Directory-Verbindung

Zum Absichern der Verbindung, zum Verhindern eines „Maskierungsangriffs“ sowie zum Schutz von LDAP-Transaktionen wird SSL-Zertifikatauthentifizierung verwendet. Die Zertifikatüberprüfung ist in Abhängigkeit von der Sicherheitsstufe, die für Ihr System erforderlich ist, optional.

## Absichern der Active Directory-Verbindung mithilfe der CLI

Die folgenden Verfahren beschreiben die Vorgehensweise zum Absichern der Active Directory-Verbindung mithilfe der CLI.

### ▼ Ausführen von Aktionen mit `getcertfile` mithilfe der CLI

`getcertfile` ist die Methode zum Hochladen einer Zertifikatdatei, falls notwendig.

- **Geben Sie zum Hochladen eines Zertifikats Folgendes ein:**

```
-> set getcertfile=tftp://IP_Adresse/Dateipfad/Dateiname
```

- **Geben Sie zum Entfernen oder Wiederherstellen eines Zertifikats Folgendes ein:**

```
-> set getcertfile=remove|restore
```

Beispiel:

```
-> set getcertfile=remove
```

Die vorhandene Zertifikatdatei, die hochgeladen wurde, wird entfernt. Die Wiederherstellung funktioniert nur, wenn zurzeit eine Zertifikatsicherungsdatei vorhanden ist. Die Absicht hierbei liegt im Speichern einer Sicherungsdatei, wenn ein Zertifikat hochgeladen wird. Sollte ein Fehler auftreten, kann die alte Datei wiederhergestellt werden.

## ▼ Aktivieren von `strictcertmode` mithilfe der CLI

`strictcertmode` ist standardmäßig deaktiviert. SSL wird zwar verwendet, aber es wird nur eine eingeschränkte Überprüfung des Zertifikats vorgenommen. Bei Aktivierung von `strictcertmode` muss das Zertifikat des Servers bereits auf den Server hochgeladen worden sein, damit die Zertifikatsignaturen überprüft werden können, wenn das Serverzertifikat während des SSL-Handshakes präsentiert wird.

- **Geben Sie zum Aktivieren des `strictcertmode` Folgendes ein:**

```
-> set strictcertmode=enabled
```

## ▼ Prüfen des `certfilestatus` mithilfe der CLI

`certfilestatus` ist eine Funktionsvariable, die den aktuellen Zertifikatstatus sowie eine Sicherungskopie des Zertifikats wiedergeben soll. Keines der beiden Elemente muss vorhanden sein, wenn `strictcertmode` deaktiviert ist. Damit der `strictcertmode` aktiviert werden kann, muss jedoch ein Zertifikat geladen sein. Das Sicherungszertifikat ist immer optional und wird nur gespeichert, wenn ein vorhandenes Zertifikat überschrieben werden soll.

- **Geben Sie zum Prüfen des Status des Zertifikats Folgendes ein:**

```
-> show /SP/clients/activedirectory certfilestatus
```

Beispiel:

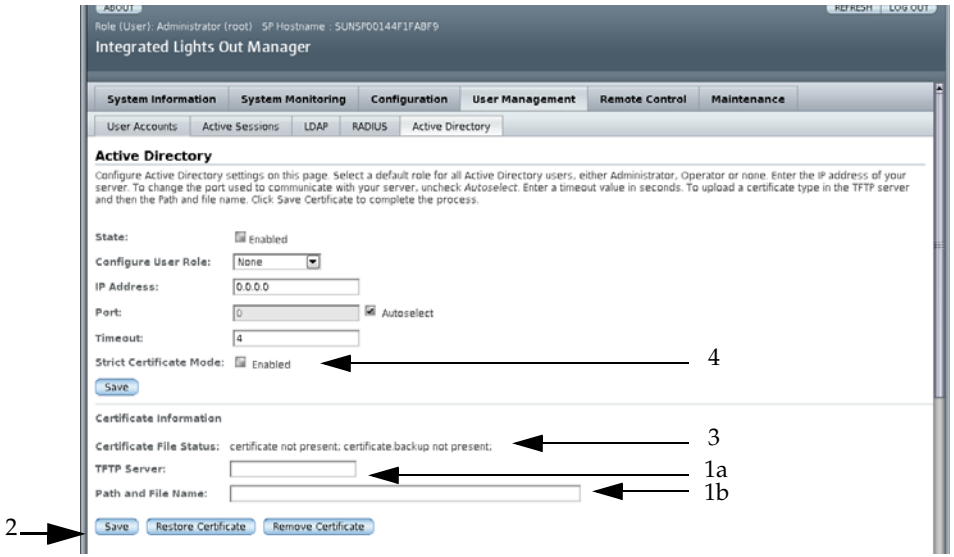
```
-> show /SP/clients/activedirectory certfilestatus
    Properties:
certfilestatus = certificate not present;certificate.backup not
present;
```

# Absichern der Active Directory-Verbindung mithilfe der Webbenutzeroberfläche

Die folgenden Verfahren beschreiben die Vorgehensweise zum Absichern der Active Directory-Verbindung mithilfe der Webbenutzeroberfläche.

ABBILDUNG 5-15 stellt die Sicherheitseigenschaften von Active Directory und die Reihenfolge, in der Daten eingegeben werden müssen, dar.

**ABBILDUNG 5-15** Sicherheitseigenschaften von Active Directory und die Reihenfolge der Dateneingabe




## ▼ Hochladen eines Zertifikats mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich bei ILOM als Benutzer mit Administratorberechtigungen an, um die Webbenutzeroberfläche zu öffnen.**
2. **Wählen Sie User Management --> Active Directory.**

   Die Seite Active Directory wird angezeigt. ABBILDUNG 5-15 illustriert die Reihenfolge, in der die Sicherheitsfelder ausgefüllt werden müssen.
3. **Geben Sie TFTP Server und Path and File Name ein. Siehe ABBILDUNG 5-15, Elemente 1a und 1b.**

4. **Klicken Sie auf die Schaltfläche Save, um die Übertragung des Zertifikats zu starten. Siehe** ABBILDUNG 5-15**, Element 2.**

---

**Hinweis –** Die Optionen zum Wiederherstellen und Entfernen stehen gegebenenfalls zur Verfügung und können ausgeführt werden, indem Sie auf die Schaltfläche Restore Certificate oder Remove Certificate klicken.

---

## ▼ Prüfen des Status der Zertifikatdatei mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich bei ILOM als Benutzer mit Administratorberechtigungen an, um die Webbenutzeroberfläche zu öffnen.**
2. **Wählen Sie User Management --> Active Directory.**

   Die Seite Active Directory wird angezeigt. Siehe ABBILDUNG 5-15, Element 3.
3. **Überprüfen Sie den Status der Zertifikatdatei.**

## ▼ Aktivieren des Strict Certificate Mode mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich bei ILOM als Benutzer mit Administratorberechtigungen an, um die Webbenutzeroberfläche zu öffnen.**
2. **Wählen Sie User Management --> Active Directory.**

   Die Seite Active Directory wird angezeigt. Siehe ABBILDUNG 5-15, Element 4.
3. **Klicken Sie auf das Kontrollkästchen neben Enable, um Strict Certificate Mode zu aktivieren.**

# LDAP (Lightweight Directory Access Protocol)

ILOM unterstützt LDAP-Authentifizierung (Lightweight Directory Access Protocol) für Benutzer auf Grundlage der OpenLDAP-Software. LDAP ist ein universeller Verzeichnisdienst. Ein Verzeichnisdienst ist eine zentrale Datenbank für verteilte Anwendungen, die auf die Verwaltung der Einträge in einem Verzeichnis ausgelegt ist. Auf diese Weise können mehrere Anwendungen gemeinsam eine einzelne Benutzerdatenbank verwenden. Weitere ausführliche Informationen zu LDAP finden Sie unter `http://www.openldap.org/`.

## Informationen zu LDAP

LDAP basiert auf einem Client/Server-Modell. LDAP stellt das Verzeichnis bereit, und die Clients greifen mithilfe des Verzeichnisdiensts auf Einträge zu. Die in einem Verzeichnis gespeicherten Daten können auf mehreren LDAP-Servern verteilt sein.

Daten sind in LDAP in einer hierarchisch Struktur organisiert, die bei einem Stamm beginnend nach unten in einzelne Einträge verzweigt. Einträge auf der obersten Ebene der Hierarchie stellen größere Organisationen dar, während sich unterhalb dieser größeren Organisationen Einträge für kleinere Organisationen befinden. Auf der untersten Ebene der Hierarchie befinden sich Einträge für einzelne Personen bzw. Ressourcen.

## LDAP-Clients und -Server

Im LDAP-Client/Server-Modell stellen LDAP-Server Informationen über Personen, Organisationen und Ressourcen den LDAP-Clients zur Verfügung. Clients nehmen mithilfe eines Clientdienstprogramms, das normalerweise im Umfang des LDAP-Servers vorhanden ist, Änderungen an der LDAP-Datenbank vor. Wird eine Änderung an der LDAP-Datenbank vorgenommen, ist diese sofort für alle Clientanwendungen sichtbar, sodass nicht jede verteilte Anwendung einzeln aktualisiert werden muss.

Um einen Eintrag im Verzeichnis beispielsweise zu aktualisieren, übermittelt ein LDAP-Client den Distinguished Name den Eintrags mit aktualisierten Attributinformationen an den LDAP-Server. Der LDAP-Server sucht den Eintrag anhand des DN (Distinguished Name) und führt einen Änderungsvorgang aus, um den Eintrag im Verzeichnis zu aktualisieren. Die aktualisierten Informationen sind sofort für alle verteilten Anwendungen verfügbar, die den betreffenden LDAP-Server verwenden.

Ein LDAP-Client kann unter anderem folgende Vorgänge ausführen:

- Suchen und Abrufen von Einträgen im bzw. aus dem Verzeichnis.
- Hinzufügen von neuen Einträgen zum Verzeichnis.
- Aktualisieren von Einträgen im Verzeichnis.
- Löschen von Einträgen im Verzeichnis.
- Umbenennen von Einträgen im Verzeichnis.

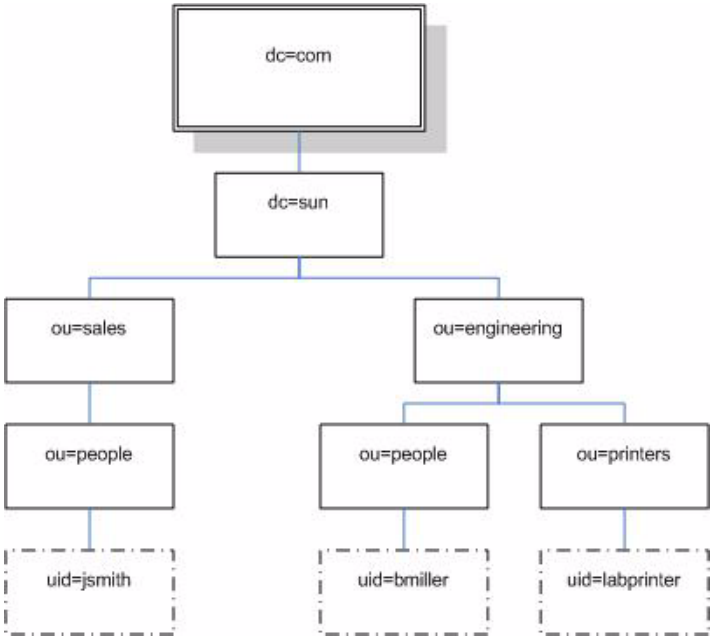
Zum Ausführen aller aufgeführten LDAP-Vorgänge muss ein LDAP-Client eine Verbindung mit einem LDAP-Server herstellen. LDAP gibt die Verwendung des TCP/IP-Anschlusses 389 an, obwohl Server über andere Anschlüsse kommunizieren können.

Ihr Server kann als Client eines LDAP-Servers eingesetzt werden. Damit LDAP-Authentifizierung verwendet werden kann, müssen Sie einen Benutzer auf Ihrem LDAP-Server erstellen, den Ihr Server authentifizieren bzw. an den er sich binden kann, sodass der Client über die Berechtigung zum Suchen des ordnungsgemäßen Verzeichnisses auf dem LDAP-Server verfügt.

# Verzeichnisorganisation auf LDAP-Servern

Daten werden in LDAP hierarchisch organisiert (siehe ABBILDUNG 5-16).

**ABBILDUNG 5-16** LDAP-Verzeichnisstruktur



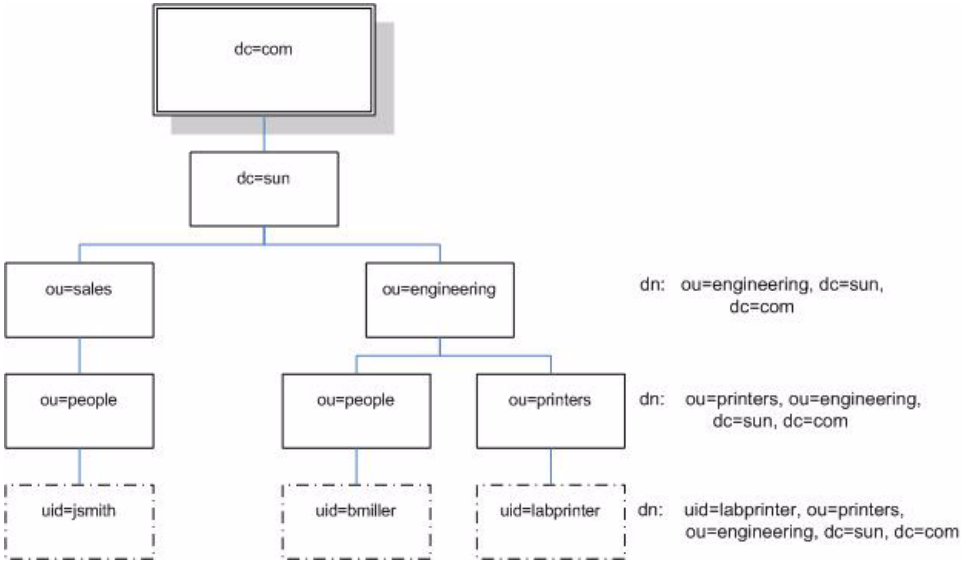
Jeder Eintrag wird eindeutig durch einen DN (Distinguished Name) identifiziert. Ein DN besteht aus einem Namen, der den Eintrag eindeutig auf der hierarchischen Stufe identifiziert, und einem Pfad, der den Eintrag bis zur Stammebene des Strukturbaums zurückverfolgt.

Der DN für jsmith lautet beispielsweise:

```
dn: uid=jsmith, ou=people, dc=sun.com
```

Hierbei steht `uid` für die Benutzer-ID-Nummer des Eintrags, `ou` für die Organisationseinheit (Organizational Unit), zu der der Eintrag gehört, und `dc` für die größere Organisation, zu der der Eintrag gehört. Das folgende Diagramm zeigt, wie Distinguished Names (DN) zum eindeutigen Identifizieren von Einträgen in der Verzeichnishierarchie verwendet werden.

**ABBILDUNG 5-17** LDAP-DNs (Distinguished Names)




# Konfigurieren von LDAP

Um LDAP verwenden zu können, müssen Sie Ihren LDAP-Server gemäß der diesem beiliegenden Dokumentation konfigurieren. Außerdem muss ILOM mithilfe der ILOM-CLI oder -Webbenutzeroberfläche konfiguriert werden.

Zur Durchführung des folgenden Verfahrens sind detaillierte Kenntnisse der eigenen LDAP-Serverkonfiguration erforderlich. Tragen Sie zuerst alle grundlegenden Netzwerkinformationen zu Ihrem LDAP-Server, einschließlich seiner IP-Adresse, zusammen, bevor Sie mit dem Verfahren beginnen.

---

**Hinweis –** Diese Aufgabe ähnelt dem Konfigurieren LDAP als Namensdienst für Linux oder Solaris.

---

## ▼ Konfigurieren des LDAP-Servers

1. **Vergewissern Sie sich, dass alle Benutzer, die bei ILOM authentifiziert werden, über Passwörter verfügen, die im Format „crypt“ oder der GNU-Erweiterung von „crypt“, gängigerweise als „MD5 crypt“ bezeichnet, gespeichert sind.**

   Beispiel:

   ```
   userPassword: {CRYPT}ajCa2He4PJhNo
   ```

   oder

   ```
   userPassword: {CRYPT}$1$pzKng1$du1Bf0NWBjh9t3FbUgf46.
   ```

   ILOM unterstützt LDAP-Authentifizierung nur für Passwörter, die in diesen beiden Varianten des crypt-Formats gespeichert sind.

2. **Fügen Sie die Objektklassen** `posixAccount` **und** `shadowAccount` **hinzu, und füllen Sie die erforderlichen Eigenschaftenwerte für dieses Schema aus (RFC 2307).**

**TABELLE 5-6** LDAP-Eigenschaftenwerte

| Erforderliche Eigenschaft | Beschreibung |
|---|---|
| uid | Benutzername zum Anmelden bei ILOM. |
| uidNumber | Beliebige eindeutige Nummer. |
| gidNumber | Beliebige eindeutige Nummer. |
| userPassword | Passwort |
| homeDirectory | Beliebiger Wert (diese Eigenschaft wird von ILOM ignoriert). |
| loginShell | Beliebiger Wert (diese Eigenschaft wird von ILOM ignoriert). |

3. **Gewähren Sie ILOM Zugriff auf die Benutzerkonten auf Ihrem LDAP-Server.**

   Aktivieren Sie entweder auf Ihrem LDAP-Server die Annahme anonymer Bindungen, oder erstellen Sie einen Proxy-Benutzer auf Ihrem LDAP-Server, der über schreibgeschützten Zugriff auf alle Benutzerkonten verfügt, die über ILOM authentifiziert werden.

   Weitere ausführliche Informationen finden Sie in Ihrer LDAP-Serverdokumentation.

## ▼ Konfigurieren von ILOM für LDAP mithilfe der CLI

1. **Geben Sie den Proxy-Benutzernamen und das Passwort ein. Geben Sie hierzu Folgendes ein:**

```
–> set /SP/clients/ldap binddn="cn=proxyuser, ou=people, ou=sales,
dc=sun, dc=com" bindpw=Passwort
```

2. **Geben Sie die IP-Adresse des LDAP-Servers ein. Geben Sie hierzu Folgendes ein:**

```
–> set /SP/clients/ldap ipaddress=LDAPIPadresse
```

3. **Weisen Sie den Anschluss zu, der für die Kommunikation mit dem LDAP-Server verwendet werden soll. Der Standardanschluss ist 389. Geben Sie hierzu Folgendes ein:**

```
–> set /SP/clients/ldap port=LDAPanschluss
```

4. **Geben Sie den Distinguished Name des Zweigs Ihrer LDAP-Struktur an, der Benutzer und Gruppen enthält. Geben Sie hierzu Folgendes ein:**

```
–> set /SP/clients/ldap searchbase="ou=people, ou=sales, dc=sun, dc=com"
```

   Hierbei handelt es sich um die Position in Ihrer LDAP-Struktur, die zur Benutzerauthentifizierung durchsucht werden soll.

5. **Legen Sie den Zustand des LDAP-Diensts auf enabled (aktiviert) fest. Geben Sie hierzu Folgendes ein:**

```
–> set /SP/clients/ldap state=enabled
```

6. **Zur Überprüfung der Funktionsfähigkeit der LDAP-Authentifizierung melden Sie sich bei ILOM mit einem LDAP-Benutzernamen und -Passwort an.**

---

**Hinweis –** ILOM durchsucht zuerst die lokalen Benutzer und dann die LDAP-Benutzer. Ist ein LDAP-Benutzername als lokaler Benutzer vorhanden, verwendet ILOM das lokale Konto für die Authentifizierung.

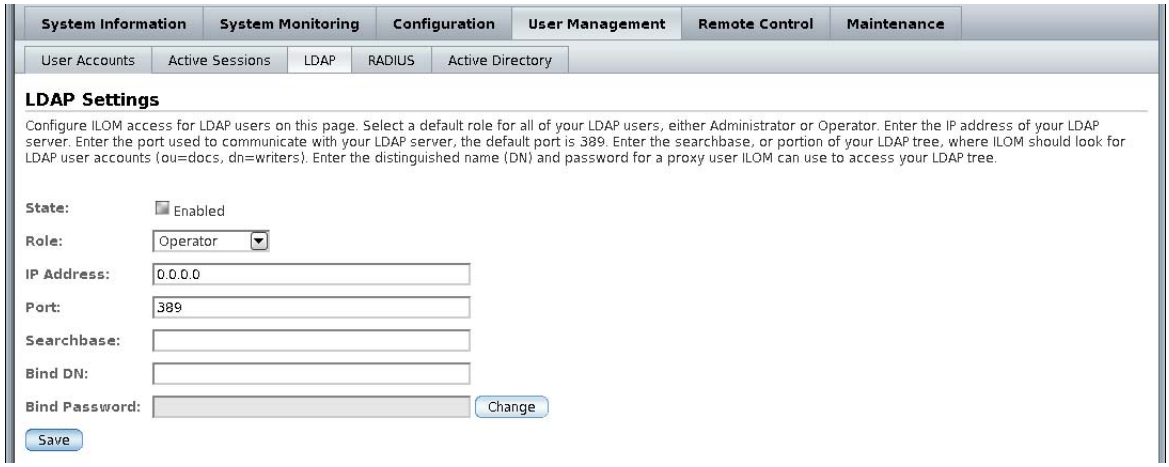
---

## ▼ Konfigurieren von ILOM für LDAP mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich bei ILOM als Administrator an, um die Webbenutzeroberfläche zu öffnen.**
2. **Wählen Sie User Management --> LDAP.**

   Die Seite LDAP Settings wird angezeigt.

**ABBILDUNG 5-18** Seite LDAP Settings


System Information
System Monitoring
Configuration
User Management
Remote Control
Maintenance
User Accounts
Active Sessions
LDAP
RADIUS
Active Directory
LDAP Settings
Configure ILOM access for LDAP users on this page. Select a default role for all of your LDAP users, either Administrator or Operator. Enter the IP address of your LDAP server. Enter the port used to communicate with your LDAP server, the default port is 389. Enter the searchbase, or portion of your LDAP tree, where ILOM should look for LDAP user accounts (ou=docs, dn=writers). Enter the distinguished name (DN) and password for a proxy user ILOM can use to access your LDAP tree.
State:
Enabled
Role:
Operator
IP Address:
0.0.0.0
Port:
389
Searchbase:
Bind DN:
Bind Password:
Change
Save

3. **Geben Sie folgende Werte ein:**

- **State** – Aktivieren Sie das Kontrollkästchen Enabled, um LDAP-Benutzer zu authentifizieren.
- **Role** – Die Standardrolle von LDAP-Benutzern. Wählen Sie im Dropdown-Listenfeld den Eintrag Administrator oder Operator.
- **IP Address** – Die IP-Adresse des LDAP-Servers.
- **Port** – Die Anschlussnummer auf dem LDAP-Server.
- **Searchbase** – Geben Sie den Zweig Ihres LDAP-Servers ein, der nach Benutzern durchsucht werden soll.
- **Bind DN** – Geben Sie den Distinguished Name (DN) eines schreibgeschützten Proxy-Benutzers auf dem LDAP-Server ein. ILOM muss über schreibgeschützten Zugriff auf Ihren LDAP-Server verfügen, um nach Benutzern suchen und diese authentifizieren zu können.
- **Bind Password** – Geben Sie das Passwort des schreibgeschützten Benutzers ein.

4. **Klicken Sie auf Save.**
5. **Zur Überprüfung der Funktionsfähigkeit der LDAP-Authentifizierung melden Sie sich bei ILOM mit einem LDAP-Benutzernamen und -Passwort an.**

**Hinweis –** ILOM durchsucht zuerst die lokalen Benutzer und dann die LDAP-Benutzer. Ist ein LDAP-Benutzername als lokaler Benutzer vorhanden, verwendet ILOM das lokale Konto für die Authentifizierung.

# RADIUS-Authentifizierung

ILOM unterstützt RADIUS-Authentifizierung (Remote Authentication Dial In User Service, DFÜ-Benutzerdienst mit entfernter Authentifizierung). RADIUS ist ein Authentifizierungsprotokoll, das die zentrale Benutzerverwaltung erleichtert. RADIUS bietet zahlreichen Servern gemeinsamen Zugriff auf Benutzerdaten in einer zentralen Datenbank, wodurch die Sicherheit erhöht und die Verwaltung vereinfacht wird. Ein RADIUS-Server kann zusammen mit mehreren RADIUS-Servern und anderen Typen von Authentifizierungsservern arbeiten.

## RADIUS-Clients und -Server

RADIUS basiert auf einem Client/Server-Modell. Der RADIUS-Server stellt die Benutzerauthentifizierungsdaten zur Verfügung und kann den Zugriff gewähren oder verweigern. Die Clients senden Benutzerdaten an den Server und empfangen eine akzeptierende oder verweigernde Antwort. Im RADIUS-Client/Server-Model sendet der Client eine Access-Request-Abfrage (Zugriffsanforderung) an den RADIUS-Server. Wenn der Server eine Access-Request-Meldung von einem Client erhält, durchsucht er die Datenbank nach den Authentifizierungsinformationen des Benutzers. Werden diese nicht gefunden, sendet der Server eine Access-Reject-Meldung (Zugriffverweigerung) und dem Benutzer wird der Zugriff auf den angeforderten Dienst verweigert. Werden die Informationen des Benutzers gefunden, antwortet der Server mit einer Access-Accept-Meldung (Zugriffsannahme). Die Access-Accept-Meldung bestätigt die Authentifizierungsdaten des Benutzers und gewährt dem Benutzer den Zugriff auf den angeforderten Dienst.

Alle Transaktionen zwischen RADIUS-Client und -Server werden unter Verwendung spezifischer Textzeichenfolgen-Passwörter, auch als „gemeinsames Geheimnis“ (shared secret) bekannt, authentifiziert. Client und Server müssen beide das Geheimnis kennen, weil es nie über das Netzwerk übertragen wird. Um RADIUS-Authentifizierung für ILOM konfigurieren zu können, müssen Sie das gemeinsame Geheimnis kennen.

Damit mit ILOM RADIUS-Authentifizierung verwendet werden kann, müssen Sie ILOM als RADIUS-Client konfigurieren.

# RADIUS-Parameter

TABELLE 5-7 In werden die RADIUS-Parameter für die Webbenutzeroberfläche und die CLI beschrieben.

**TABELLE 5-7** RADIUS-Einstellungen für Webbenutzeroberfläche und CLI

| Webbenutzeroberfläche | CLI | Beschreibung |
|---|---|---|
| State | `state` *enabled*\|*disabled* | Muss für die Authentifizierung von RADIUS-Benutzern aktiviert sein. |
| Role | `defaultrole` *administrator*\|*operator* | Legt die Standardrolle für alle RADIUS-Benutzer fest – Administrator oder Operator. |
| IP Address | `ipaddress` *IPadresse* | Die IP-Adresse des RADIUS-Servers. |
| Port | `port` *Anschlussnum* | Die für die Kommunikation mit dem RADIUS-Server verwendete Anschlussnummer. Der Standardanschluss ist 1812. |
| Shared Secret | `secret` *Text* | Das gemeinsame Geheimnis, mit dem der Zugriff auf RADIUS erhalten wird. |

# Konfigurieren von RADIUS-Einstellungen

Wenn Sie ILOM Zugriff auf mehr als die 10 lokalen Benutzerkonten gewähren müssen und dies, nachdem der RADIUS-Server ordnungsgemäß konfiguriert wurde, können Sie ILOM so konfigurieren, dass RADIUS-Authentifizierung verwendet wird.

Tragen Sie vor dem Durchführen dieses Verfahrens zuerst alle erforderlichen Informationen zu Ihrer RADIUS-Umgebung, wie sie unter „Verwalten von Benutzerkonten“ auf Seite 63 beschrieben sind, zusammen.

## ▼ Konfigurieren von RADIUS mithilfe der CLI

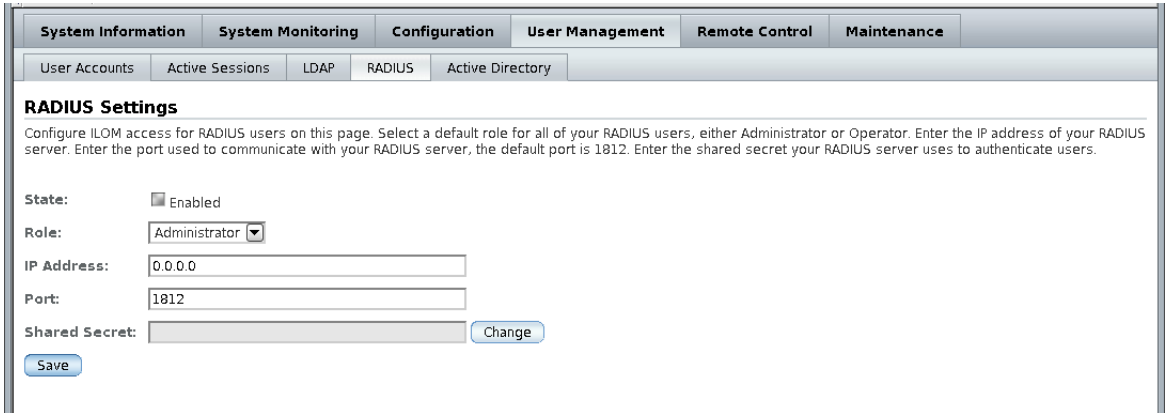
1. **Melden Sie sich bei der ILOM-CLI als Benutzer mit Administratorberechtigungen an.**
2. **Wechseln Sie nach** `/SP/clients/radius`**. Siehe** „RADIUS-Befehle“ auf Seite 103**.**
3. **Legen Sie die in** TABELLE 5-7 **dargestellten Parameter fest.**

## ▼ Konfigurieren von RADIUS mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich bei ILOM als Administrator an, um die Webbenutzeroberfläche zu öffnen.**
2. **Wählen Sie User Management --> RADIUS.**

   Die Seite RADIUS Settings wird angezeigt.

**ABBILDUNG 5-19** Seite RADIUS Settings




3. **Nehmen Sie die Einstellungen vor.**

   Ausführliche Informationen finden Sie unter TABELLE 5-7
4. **Klicken Sie auf Save, um die Änderungen zu übernehmen.**

# RADIUS-Befehle

In diesem Abschnitt werden die RADIUS-Befehle beschrieben.

## `show /SP/clients/radius`

Dieser Befehl ist für Administratoren und Operatoren verfügbar.

### *Funktion*

Mit diesem Befehl können die der RADIUS-Authentifizierung zugeordneten Eigenschaften angezeigt werden.

### *Syntax*

```
show /SP/clients/radius
```

### *Eigenschaften*

`defaultrole` – Die allen RADIUS-Benutzern zugewiesene Rolle: Administrator oder Operator.

`ipaddress` – Die IP-Adresse Ihres RADIUS-Servers.

`port` – Die für die Kommunikation mit Ihrem RADIUS-Server verwendete Anschlussnummer. Der Standardanschluss ist 1812.

`secret` – Das gemeinsame Geheimnis, mit dem der Zugriff auf Ihren RADIUS-Server erhalten wird.

`state` – Diese Einstellung ist aktiviert oder deaktiviert, um den Zugriff auf Ihre RADIUS-Benutzer zu gewähren oder zu verweigern.

### *Beispiel*

```
 -> show /SP/clients/radius

   /SP/clients/radius
    Targets:

    Properties:
        defaultrole = Operator
        ipaddress = 129.144.36.142
        port = 1812
        secret = (none)
        state = enabled

    Commands:
        cd
        set
        show

->
```

## set /SP/clients/radius

Dieser Befehl ist für Administratoren verfügbar.

### *Funktion*

Mit diesem Befehl können die der RADIUS-Authentifizierung zugeordneten Eigenschaften auf einem Service-Prozessor (SP) konfiguriert werden.

### *Syntax*

```
set /SP/clients/radius [defaultrole=[Administrator|Operator]
ipaddress=radiusserverIP port=port# secret=radiussecret state=
[enabled|disabled]]
```

### *Eigenschaften*

- `defaultrole` – Sie müssen eine Berechtigungsstufe zuweisen, die für alle RADIUS-Benutzer zutrifft – Administrator oder Operator.
- `ipaddress` – Die IP-Adresse Ihres RADIUS-Servers.
- `port` – Die für die Kommunikation mit Ihrem RADIUS-Server verwendete Anschlussnummer. Der Standardanschluss ist 1812.
- `secret` – Geben Sie das gemeinsame Geheimnis ein, mit dem der Zugriff auf Ihren RADIUS-Server erhalten wird. Wird auch als Verschlüsselungsschlüssel bezeichnet.
- `state` – Wählen Sie „enabled“ oder „disabled“, um den Zugriff auf Ihre RADIUS-Benutzer zu gewähren oder zu verweigern.

### *Beispiel*

```
  -> set /SP/clients/radius state=enabled ipaddress=10.8.145.77
Set 'state' to 'enabled'
Set 'ipaddress' to '10.8.145.77
```

## show /SP/clients

Dieser Befehl ist für Administratoren und Operatoren verfügbar.

### *Funktion*

Mit diesem Befehl können Sie Clients anzeigen, die Daten von einem Service-Prozessor empfangen können, einschließlich LDAP-, NTP-, RADIUS- und SYSLOG-Clients.

### *Syntax*

```
show /SP/clients
```

*Beispiel*

```
-> show /SP/clients

 /SP/clients
   Targets:
 ldap
 ntp
 radius
 syslog

   Properties:

   Commands:
       cd
       show
```

---

**Hinweis –** Benutzer mit Operatorberechtigungen können nur die `ntp`- und `syslog`-Ziele anzeigen. Die `radius`- und `ldap`-Ziele bleiben ausgeblendet.

---

KAPITEL 6

# Bestands- und Komponentenverwaltung

Mithilfe von ILOM können Sie Komponentendetails wie den Namen, Typ und Fehlerstatus der Komponente anzeigen. Zusätzlich können Sie mit ILOM das Entfernen und Installieren von Komponenten vorbereiten.

Dieses Kapitel enthält folgende Abschnitte:


- „Anzeigen von Komponenteninformationen und Verwalten des Bestands“ auf Seite 108
  - „Anzeigen von Komponenteninformationen mithilfe der CLI“ auf Seite 108
  - „Anzeigen von Komponenteninformationen mithilfe der Webbenutzeroberfläche“ auf Seite 109
- „Ausführen einer Aktion mit einer Komponente“ auf Seite 110
  - „Vorbereiten des Entfernens einer Komponente mithilfe der CLI“ auf Seite 111
  - „Ermitteln der Bereitschaft einer Komponente zum Entfernen mithilfe der CLI“ auf Seite 111
  - „Wiederinbetriebnehmen einer Komponente mithilfe der CLI“ auf Seite 112
  - „Vorbereiten des Entfernens einer Komponente mithilfe der Webbenutzeroberfläche“ auf Seite 112
  - „Wiederinbetriebnehmen einer Komponente mithilfe der Webbenutzeroberfläche“ auf Seite 113
- „Aktivieren und Deaktivieren von Komponenten“ auf Seite 114
  - „Aktivieren und Deaktivieren von Komponenten mithilfe der CLI“ auf Seite 114
  - „Aktivieren und Deaktivieren von Komponenten mithilfe der Webbenutzeroberfläche“ auf Seite 114
- „Konfigurieren von Richtlinieneinstellungen“ auf Seite 115
  - „Konfigurieren von Richtlinieneinstellungen mithilfe der CLI“ auf Seite 115
  - „Konfigurieren von Richtlinieneinstellungen mithilfe der Webbenutzeroberfläche“ auf Seite 116

**Hinweis –** In diesem Kapitel verwendete Syntaxbeispiele verwenden das Ziel beginnend mit `/SP/`. Dies könnte in Abhängigkeit von der verwendeten Serverplattform gegen das Ziel beginnend mit `/CMM/` ausgetauscht werden. Unterziele sind auf allen Serverplattformen gleich.

# Anzeigen von Komponenteninformationen und Verwalten des Bestands

Die folgenden Verfahren erläutern, wie Komponenteninformationen angezeigt werden. Sowohl Administratoren als auch Operatoren dürfen Komponenteninformationen anzeigen.

## ▼ Anzeigen von Komponenteninformationen mithilfe der CLI

1. **Melden Sie sich bei der ILOM-CLI als Administrator oder Operator an.**
2. **Geben Sie an der Befehlseingabeaufforderung Folgendes ein:**

```
-> show komponenten_name type
```

Beispiel:

```
-> show /SYS/MB type
    Properties:
        type = Motherboard
    Commands:
        show
```

Die Eigenschaften, die Bestandsinformationen enthalten, sind in der folgenden Liste dargestellt. Welche der Eigenschaften von Ihnen angezeigt werden können, hängt vom verwendeten Zieltyp ab.

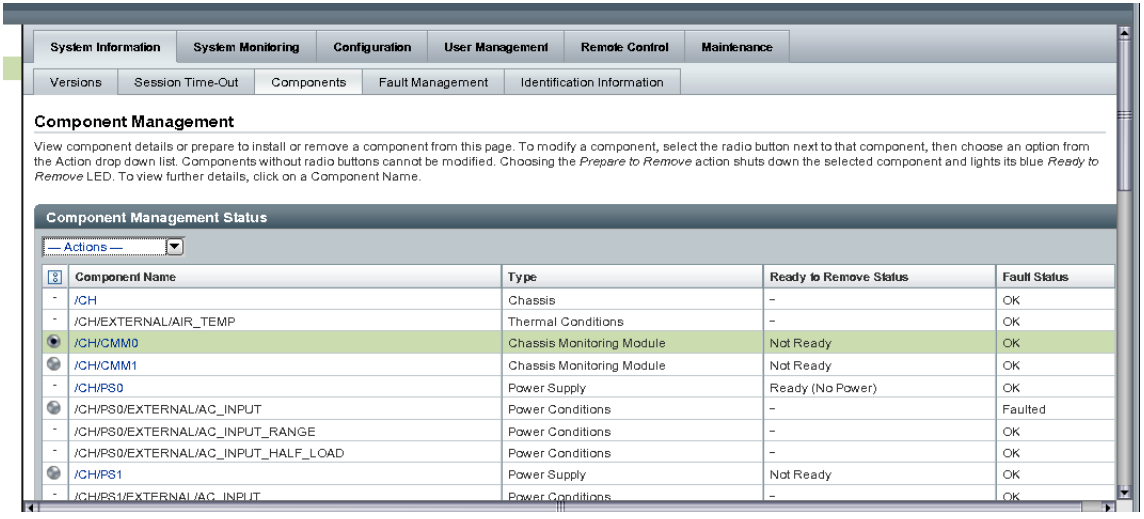
- `fru_part_number`
- `fru_manufacturer`
- `fru_serial_number`

- fru_name
- fru_description
- fru_version
- chassis_serial_number
- chassis_part_number
- product_name
- product_serial_number
- product_part_number
- customer_frudata

## ▼ Anzeigen von Komponenteninformationen mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich bei der ILOM-Webbenutzeroberfläche als Administrator oder Operator an.**
2. **Wählen Sie System Information -> Components.**
   Die Seite Component Management wird angezeigt.

**ABBILDUNG 6-1** Seite Component Management



3. **Klicken Sie auf den Namen einer Komponente in der Tabelle Component Management Status.**

   Ein Dialogfeld mit Informationen zu der ausgewählten Komponente wird angezeigt.

**ABBILDUNG 6-2** Dialogfeld Component Information

# Ausführen einer Aktion mit einer Komponente

Über das Anzeigen von Bestandsinformationen hinaus können Sie außerdem folgende Aktionen mit Komponenten durchführen:

- Vorbereiten des Entfernens bzw. der Wiederinbetriebnahme – Siehe „Entfernen und Austauschen von Komponenten“ auf Seite 111.
- Aktivieren/Deaktivieren – Siehe „Aktivieren und Deaktivieren von Komponenten“ auf Seite 114.
- Beseitigen von Fehlern – Siehe „Fehlerverwaltung“ auf Seite 129.

# Entfernen und Austauschen von Komponenten

Zahlreiche Komponenten können im laufenden Betrieb des Systems ausgetauscht werden, indem ein Verfahren zum Entfernen und Austauschen verwendet wird. Das Verfahren beinhaltet das Entfernen und Einsetzen von Modulen in das System. Vor dem Entfernen eines Moduls aus einem System müssen Sie das Modul mithilfe der ILOM-CLI oder -Webbenutzeroberfläche vorbereiten.

## ▼ Vorbereiten des Entfernens einer Komponente mithilfe der CLI

1. **Melden Sie sich bei der ILOM-CLI als Administrator oder Operator an.**
2. **Geben Sie an der ILOM-Befehlseingabeaufforderung Folgendes ein:**

```
–> set <Ziel> prepare_to_remove_action=true
```

Beispiel:

```
-> set /CH/RFM0 prepare_to_remove_action=true
Set 'prepare_to_remove_action' to 'true'
```

## ▼ Ermitteln der Bereitschaft einer Komponente zum Entfernen mithilfe der CLI

Nachdem die Komponente zum Entfernen vorbereitet wurde, können Sie überprüfen, ob sie bereit ist, um physikalisch entfernt zu werden.

1. **Melden Sie sich bei der ILOM-CLI als Administrator oder Operator an.**
2. **Geben Sie an der ILOM-Befehlseingabeaufforderung Folgendes ein:**

```
–> show <Ziel> prepare_to_remove_status
```

Beispiel:

```
 -> show /CH/RFM0 prepare_to_remove_status
    Properties:
        prepare_to_remove_status = Ready|NotReady
    Commands:
        cd
        set
        show
        start
        stop
```

Die `Ready|NotReady`-Anweisung in dem Beispiel zeigt an, ob das Gerät zum Entfernen bereit ist.

## ▼ Wiederinbetriebnehmen einer Komponente mithilfe der CLI

Wenn eine Komponente bereits zum Entfernen vorbereitet wurde, dieser Vorgang aber rückgängig gemacht werden soll, kann dies von einem entfernten Standort aus erfolgen.

1. **Melden Sie sich bei der ILOM-CLI als Administrator oder Operator an.**
2. **Geben Sie an der ILOM-Befehlseingabeaufforderung Folgendes ein:**

```
–> set <Ziel> return_to_service_action=true
```

Beispiel:

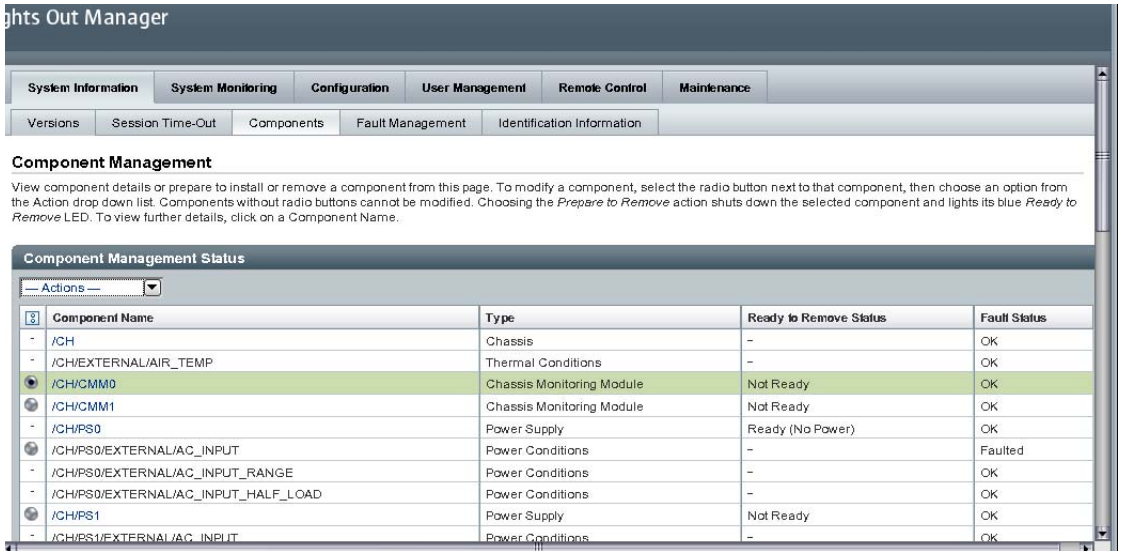
```
-> set /CH/RFM0 return_to_service_action=true
Set 'return_to_service_action' to 'true'
```

## ▼ Vorbereiten des Entfernens einer Komponente mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich bei der ILOM-Webbenutzeroberfläche als Administrator oder Operator an.**
2. **Wählen Sie System Information -> Components.**

   Die Seite Component Management wird angezeigt.

**ABBILDUNG 6-3** Seite Component Management




3. **Aktivieren Sie das Optionsfeld neben der Komponente, die entfernt werden soll.**

   Komponenten ohne Optionsfelder können nicht entfernt werden.

4. **Wählen Sie im Dropdown-Listenfeld Actions den Eintrag Prepare to Remove.**

## ▼ Wiederinbetriebnehmen einer Komponente mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich bei der ILOM-Webbenutzeroberfläche als Administrator oder Operator an.**

2. **Wählen Sie System Information -> Components.**

   Die Seite Component Management wird angezeigt.

3. **Aktivieren Sie das Optionsfeld neben der Komponente, die wieder in Betrieb genommen werden soll.**

4. **Wählen Sie im Dropdown-Listenfeld Actions den Eintrag Return to Service.**

# Aktivieren und Deaktivieren von Komponenten

In Abhängigkeit von der Serverplattform können Sie möglicherweise bestimmte Komponenten aktivieren bzw. deaktivieren. Weitere ausführliche Informationen finden Sie in der spezifischen Dokumentation, die der jeweiligen Serverplattform beiliegt.

## ▼ Aktivieren und Deaktivieren von Komponenten mithilfe der CLI

1. **Melden Sie sich bei der ILOM-CLI als Administrator an.**
2. **Geben Sie an der ILOM-Befehlseingabeaufforderung Folgendes ein:**

```
-> set /SYS/MB/CMP0/P0/C0 component_state=enabled | disabled
```

## ▼ Aktivieren und Deaktivieren von Komponenten mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich bei der ILOM-Webbenutzeroberfläche als Administrator an.**
2. **Wählen Sie System Information -> Components.**
   Die Seite Component Management wird angezeigt.
3. **Aktivieren Sie das Optionsfeld neben der Komponente, die aktiviert bzw. deaktiviert werden soll.**
4. **Wählen Sie im Dropdown-Listenfeld Actions den Eintrag Enable oder Disable.**
   In Abhängigkeit von Ihrer Auswahl wird die Komponente aktiviert bzw. deaktiviert.

# Konfigurieren von Richtlinieneinstellungen

Richtlinien sind Einstellungen, die das Verhalten des Systems steuern. Richtlinien sind in den Standardeinstellungen des Systems enthalten und können einfach mithilfe der ILOM-CLI oder -Webbenutzeroberfläche geändert werden.

## ▼ Konfigurieren von Richtlinieneinstellungen mithilfe der CLI

1. **Melden Sie sich bei der ILOM-CLI als Administrator an.**
2. **Geben Sie an der ILOM-Befehlseingabeaufforderung Folgendes ein:**

```
—> show /CMM/policy
```

Beispiel

```
 -> show /CMM/policy
  /CMM/policy
     Targets:
     Properties:
 Policy1Name = enabled
 Policy2Name = enabled
 Policy2Name = enabled
     Commands:
          cd
          set
          show
```

3. **Geben Sie an der ILOM-Befehlseingabeaufforderung Folgendes ein:**

```
—> set /CMM/policy
```

Beispiel

```
-> set /CMM/Policy1Name=enabled
/CMM/Policy1Name=enabled
```

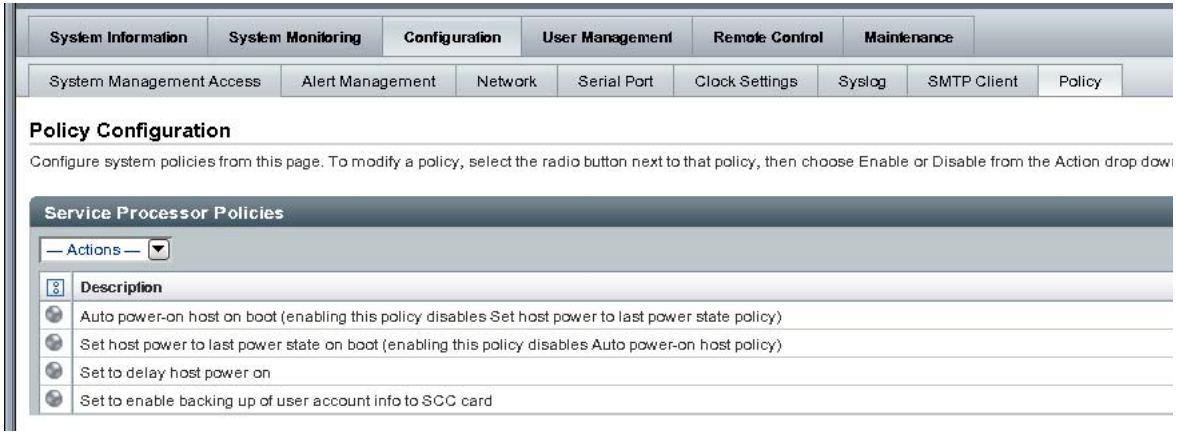
## ▼ Konfigurieren von Richtlinieneinstellungen mithilfe der Webbenutzeroberfläche

Je nach der verwendeten Serverplattform können Sie möglicherweise Richtlinieneinstellungen konfigurieren.

1. **Melden Sie sich bei der ILOM-Webbenutzeroberfläche als Administrator an.**
2. **Wählen Sie Configuration --> Policy.**

   Das Fenster Policy Configuration wird angezeigt.
3. **Aktivieren Sie das Optionsfeld neben der Richtlinie, die geändert werden soll.**
4. **Wählen Sie im Dropdown-Listenfeld Actions den Eintrag Enable oder Disable.**

**ABBILDUNG 6-4** Seite Policy Configuration


System Information
System Monitoring
Configuration
User Management
Remote Control
Maintenance
System Management Access
Alert Management
Network
Serial Port
Clock Settings
Syslog
SMTP Client
Policy
Policy Configuration
Configure system policies from this page. To modify a policy, select the radio button next to that policy, then choose Enable or Disable from the Action drop dow
Service Processor Policies
— Actions —
Description
Auto power-on host on boot (enabling this policy disables Set host power to last power state policy)
Set host power to last power state on boot (enabling this policy disables Auto power-on host policy)
Set to delay host power on
Set to enable backing up of user account info to SCC card

KAPITEL 7

# Systemüberwachung und Alarmverwaltung

Mithilfe der Systemüberwachungsfunktionen in ILOM können Sie den Zustand des Systems proaktiv überwachen. Die Alarmüberwachungsfunktionen in ILOM ermöglichen Ihnen das Empfangen von Vorabbenachrichtigungen über Ereignisse, die im System auftreten. Die Systemüberwachungs- und Alarmverwaltungsfunktionen in ILOM können über die ILOM-Webbenutzeroberfläche oder die CLI angezeigt und verwaltet werden.

Dieses Kapitel enthält folgende Themen:


- „Informationen zur Systemüberwachung“ auf Seite 118
  - „Sensormesswerte“ auf Seite 119
  - „System-LEDs“ auf Seite 123
  - „ILOM-Ereignisprotokoll“ auf Seite 126
  - „Ereignisprotokoll-Zeitstempel und ILOM-Zeiteinstellungen“ auf Seite 127
  - „Syslog-Informationen“ auf Seite 128
  - „Fehlerverwaltung“ auf Seite 129
- „Überwachen von Systemsensoren, LEDs und des ILOM-Ereignisprotokolls“ auf Seite 132
  - „Ermitteln des Zustands von LEDs mithilfe der Webbenutzeroberfläche“ auf Seite 132
  - „Ermitteln von Sensormesswerten mithilfe der Webbenutzeroberfläche“ auf Seite 133
  - „Anzeigen und Löschen des ILOM-Ereignisprotokolls mithilfe der Webbenutzeroberfläche“ auf Seite 134
  - „Anzeigen und Löschen des ILOM-Ereignisprotokolls mithilfe der CLI“ auf Seite 136
  - „Anzeigen und Festlegen von Zeiteinstellungen mithilfe der CLI“ auf Seite 128

- „Anzeigen und Konfigurieren von Zeiteinstellungen mithilfe der Webbenutzeroberfläche“ auf Seite 138
- „Konfigurieren von IP-Adressen von entfernten Syslog-Empfängern mithilfe der Webbenutzeroberfläche“ auf Seite 139
- „Konfigurieren von IP-Adressen von entfernten Syslog-Empfängern mithilfe der CLI“ auf Seite 140

- „Informationen zur Alarmverwaltung“ auf Seite 141
  - „Konfiguration von Alarmregeln“ auf Seite 141
  - „Definitionen von Alarmregeleigenschaften“ auf Seite 142
- „Verwalten von Alarmregelkonfigurationen mithilfe der ILOM-Webbenutzeroberfläche“ auf Seite 145
  - „Voraussetzungen“ auf Seite 146
  - „Ändern von Alarmregelkonfigurationen mithilfe der Webbenutzeroberfläche“ auf Seite 146
  - „Deaktivieren von Alarmregelkonfigurationen mithilfe der Webbenutzeroberfläche“ auf Seite 147
  - „Erzeugen von Alarmtests mithilfe der Webbenutzeroberfläche“ auf Seite 148
- „Verwalten von Alarmregelkonfigurationen mithilfe der ILOM-CLI“ auf Seite 149
  - „CLI-Befehle zum Verwalten von Alarmregelkonfigurationen“ auf Seite 150
  - „Ändern von Alarmregelkonfigurationen mithilfe der CLI“ auf Seite 152
  - „Deaktivieren von Alarmregelkonfigurationen mithilfe der CLI“ auf Seite 153
- „Konfigurieren eines SMTP-Clients für E-Mail-Benachrichtigungsalarme“ auf Seite 155
  - „Aktivieren eines SMTP-Clients mithilfe der Webbenutzeroberfläche“ auf Seite 156
  - „Aktivieren eines SMTP-Clients mithilfe der CLI“ auf Seite 156


# Informationen zur Systemüberwachung

Die Systemüberwachungsfunktionen in ILOM ermöglichen die einfache Ermittlung des Zustands des Systems sowie die schnelle Erkennung von Fehlern bei deren Auftreten. So haben Sie in ILOM beispielsweise folgende Möglichkeiten:

- Ermitteln unmittelbarer Sensormesswerte zu Temperaturen, Stromstärke, Spannung, Lüftergeschwindigkeit und Vorhandensein von Systemkomponenten. Weitere Informationen zu diesem Thema finden Sie unter „Sensormesswerte“ auf Seite 119.

- Ermitteln des Zustands von LEDs innerhalb des Systems. Weitere Informationen zu diesem Thema finden Sie unter „System-LEDs“ auf Seite 123.
- Identifizieren von Systemfehlern und Anzeigen von Ereignisinformationen im ILOM-Ereignisprotokoll. Weitere Informationen zu diesem Thema finden Sie unter „ILOM-Ereignisprotokoll“ auf Seite 126.
- Anzeigen des Fehlerzustands einer Systemkomponente. Weitere Informationen zu diesem Thema finden Sie unter „Fehlerverwaltung“ auf Seite 129.
- Empfangen erzeugter Benachrichtigungen über Systemereignisse im Voraus über IPMI PET-Alarme, SNMP-Trap-Alarme oder per E-Mail-Benachrichtigungsalarme. Weitere Informationen zu diesem Thema finden Sie unter „Informationen zur Alarmverwaltung“ auf Seite 141.

## Sensormesswerte

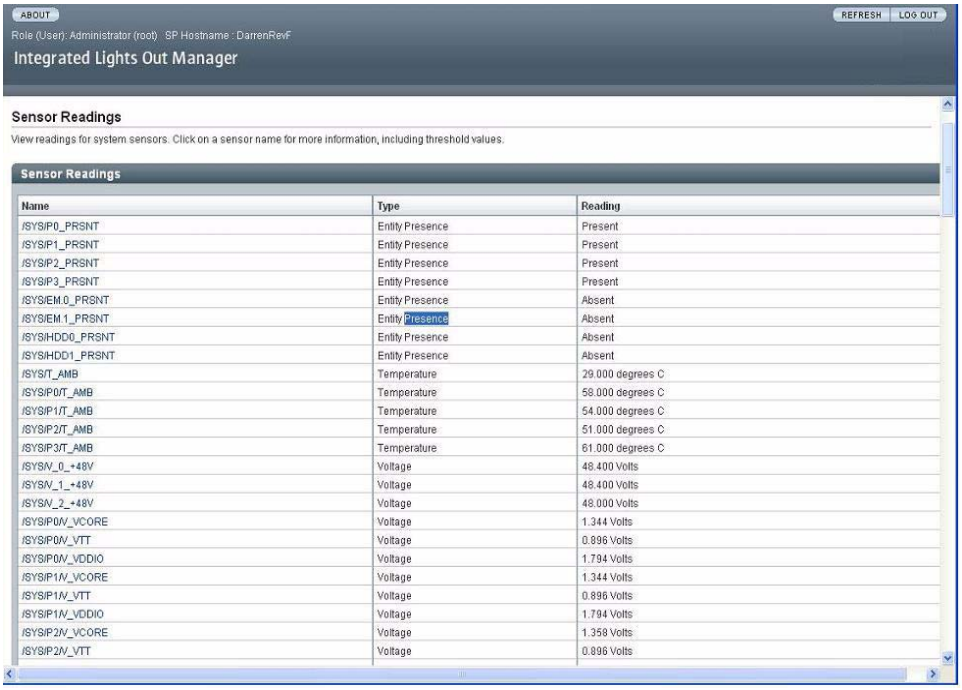
Alle Serverplattformen sind mit einer Anzahl von Sensoren ausgestattet, die die Spannung, Temperaturen, Lüftergeschwindigkeiten und andere Eigenschaften des Systems messen. In ILOM enthält jeder Sensor neun Eigenschaften, die verschiedene Einstellungen in Bezug auf einen Sensor beschreiben, z. B. Sensortyp, Sensorklasse, Sensorwert sowie die Sensorwerte für obere und untere Schwellenwerte.

ILOM ruft die Sensoren im System regelmäßig ab und meldet alle Ereignisse im Zusammenhang mit Änderungen von Sensorzuständen oder dem Überschreiten von Sensorschwellenwerten an das ILOM-Ereignisprotokoll. Zusätzlich erzeugt ILOM automatisch eine Alarmmeldung an das definierte Alarmziel, wenn eine Alarmregel im System aktiviert ist, die dem überschrittenen Schwellenwert entspricht.

# Ermitteln von Sensormesswerten mithilfe der Webbenutzeroberfläche

In der ILOM-Webbenutzeroberfläche erhalten Sie unmittelbare Sensormesswerte über System-FRUs (Field Replaceable Units) oder andere Systembestandteile auf der Seite System Monitoring --> Sensor Readings.

**ABBILDUNG 7-1** Seite Sensor Readings


ABOUT
REFRESH
LOG OUT
Role (User): Administrator (root) SP Hostname : DarrenRevF
Integrated Lights Out Manager
Sensor Readings
View readings for system sensors. Click on a sensor name for more information, including threshold values.
Sensor Readings
Name
Type
Reading
/SYS/P0_PRSNT Entity Presence Present
/SYS/P1_PRSNT Entity Presence Present
/SYS/P2_PRSNT Entity Presence Present
/SYS/P3_PRSNT Entity Presence Present
/SYS/EM.0_PRSNT Entity Presence Absent
/SYS/EM.1_PRSNT Entity Presence Absent
/SYS/HDD0_PRSNT Entity Presence Absent
/SYS/HDD1_PRSNT Entity Presence Absent
/SYS/T_AMB Temperature 29.000 degrees C
/SYS/P0/T_AMB Temperature 58.000 degrees C
/SYS/P1/T_AMB Temperature 54.000 degrees C
/SYS/P2/T_AMB Temperature 51.000 degrees C
/SYS/P3/T_AMB Temperature 61.000 degrees C
/SYS/V_0_+48V Voltage 48.400 Volts
/SYS/V_1_+48V Voltage 48.400 Volts
/SYS/V_2_+48V Voltage 48.000 Volts
/SYS/P0/V_VCORE Voltage 1.344 Volts
/SYS/P0/V_VTT Voltage 0.896 Volts
/SYS/P0/V_VDDIO Voltage 1.794 Volts
/SYS/P1/V_VCORE Voltage 1.344 Volts
/SYS/P1/V_VTT Voltage 0.896 Volts
/SYS/P1/V_VDDIO Voltage 1.794 Volts
/SYS/P2/V_VCORE Voltage 1.358 Volts
/SYS/P2/V_VTT Voltage 0.896 Volts

Auf der Seite Sensor Readings werden die Messwerte für jeden Sensor nach Name, Typ und Messwert aufgeführt. Weitere Informationen zu einem Schwellenwertsensor erhalten Sie, indem Sie auf der Seite auf den Namen eines Schwellenwertsensors klicken, um weitere Schwellenwerteigenschaften anzuzeigen. Wenn Sie beispielsweise auf den Schwellenwertsensornamen `/SYS/T_AMB` klicken, wird folgendes Dialogfeld mit zusätzlichen Informationen zu diesem Sensor angezeigt.

**ABBILDUNG 7-2** Dialogfeld mit Sensoreigenschaften für `/SYS/T_AMB`

Weitere Informationen zum Ermitteln von Sensormesswerten in der ILOM-Webbenutzeroberfläche finden Sie unter „Ermitteln des Zustands von LEDs mithilfe der Webbenutzeroberfläche“ auf Seite 132.

## Ermitteln von Sensormesswerten mithilfe der CLI

In der ILOM-CLI erhalten Sie unmittelbare Sensormesswerte über System-FRUs und andere Systembestandteile innerhalb des Namespace `/SYS` oder `/CH`. Beide Namespaces unterstützen zwei Klassen von Sensormesswerten, auf die Sie zugreifen können. Diese Klassen sind *Schwellenwertsensormesswerte* und *Diskrete Sensormesswerte*. Eine kurze Zusammenfassung, in der beide Klassen beschrieben werden, finden Sie im Folgenden.

### *Schwellenwertsensoren*

Schwellenwertsensoren bieten einen Sensoreigenschaftenwert sowie vordefinierte kritische und nicht kritische obere und untere Schwellenwerte. Schwellenwertsensoren umfassen normalerweise Temperatur-, Spannungs- und Lüftermesswerte.

Zur Ermittlung von Sensormesswerten mithilfe der ILOM-CLI müssen Sie mit dem Befehl `cd` zum Sensorziel navigieren und dann mit dem Befehl `show` die Sensoreigenschaften anzeigen.

Auf einigen Serverplattformen können Sie beispielsweise den folgenden Pfad angeben, um einen Temperaturmesswert der Leistungsaufnahme eines Servers zu erhalten:

```
cd /SYS/T_AMB
show
```

Die das Sensorziel beschreibenden Eigenschaften werden angezeigt. Beispiel:

- `Type = Sensor`
- `Class = Threshold Sensor`
- `Value = 32.000 degree C`
- `Upper = non-recov_threshold = 80.00 degree C`
- `Upper critical_threshold = 75.00 degree C`
- `Upper noncritical_threshold = 70.00 degree C`
- `Lower non_recov_threshold = 0.00 degree C`
- `Lower critical_threshold = 0.00 degree C`
- `Lower noncritical_threshold = 0.00 degree C`

Spezifische Detailinformationen zu den Typen von Schwellenwertsensorzielen, die verfügbar sind, sowie deren Zugriffspfade finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

### *Diskrete Sensoren*

Diskrete Sensoren bieten einen Satz genau definierter Werte, der dem jeweiligen Sensorziel zugeordnet ist. Diskrete Sensoren bieten normalerweise Informationen über das Vorhandensein oder Versagen einer Einheit oder den Zustand einer Stromversorgung.

Zur Ermittlung eines diskreten Sensormesswerts mithilfe der ILOM-CLI müssen Sie mit dem Befehl `cd` zum Sensorziel navigieren und dann mit dem Befehl `show` die Zieleigenschaften anzeigen. Auf Serverplattformen können Sie beispielsweise ermitteln, ob ein Festplattenlaufwerk in Steckplatz 0 vorhanden ist, indem Sie folgenden Pfad angeben:

```
cd /SYS/HDD0_PRSNT
show
```

Die das diskrete Sensorziel beschreibenden Eigenschaften werden angezeigt. Beispiel:

- `Type = Entity Presence`
- `Class = Discrete Indicator`
- `Value = Present`

Spezifische Detailinformationen zu den Typen von diskreten Sensorzielen, die verfügbar sind, sowie deren Zugriffspfade finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

# System-LEDs

System-LEDs werden normalerweise am System von ILOM auf Grundlage der Serverplattformrichtlinie aktiviert. Üblicherweise leuchten die System-LEDs durch ILOM auf, wenn einer der folgenden Zustände eintritt:

- Versagen bzw. Fehler in einer Komponente wurde erkannt.
- FRU (Field Replaceable Unit) benötigt Wartung.
- Hot-Plug-Modul ist zum Entfernen bereit.
- Aktivität in einem FRU oder System.

Die Zustände von System-LEDs können über die ILOM-Webbenutzeroberfläche oder die ILOM-CLI angezeigt werden. Darüber hinaus können Sie in manchen Fällen eventuell den Zustand einer System-LED ändern.

## Unterstützte Zustände von System-LEDs

ILOM unterstützt die folgenden Zustände von System-LEDs:

- **Aus (Off)** – Normaler Betriesbzustand. Kein Eingreifen erforderlich.
- **Dauerleuchten (Steady On)** – Komponente ist zum Entfernen bereit.
- **Langsames Blinken (Slow Blink)** – Komponente ändert ihren Zustand.
- **Schnelles Blinken (Fast Blink)** – Hilft beim Auffinden des Systems in einem Rechenzentrum.
- **Standby-Blinken (Standby Blink)** – Komponente ist zur Aktivierung bereit, aber im Moment noch nicht funktionsbereit.

### *Typen von Zuständen von System-LEDs*

ILOM unterstützt zwei Typen von Zuständen von System-LEDs: *Veränderbar* und *Vom System zugewiesen*.

- **Veränderbare Zustände** – Einige System-LEDs in ILOM bieten veränderbare Zustände. Normalerweise stellen diese Typen von System-LEDs Betriebszustände verschiedener Systemkomponenten zur Verfügung Der Typ der dargestellten Zustände wird über die System-LED bestimmt. Beispielsweise können in Abhängigkeit von der System-LED die folgenden veränderbaren Zustände vorhanden sein:
  - **Aus (Off)** – Normaler Betriesbzustand. Kein Eingreifen erforderlich.
  - **Schnelles Blinken (Fast Blink)** – Hilft beim Auffinden des Systems in einem Rechenzentrum.

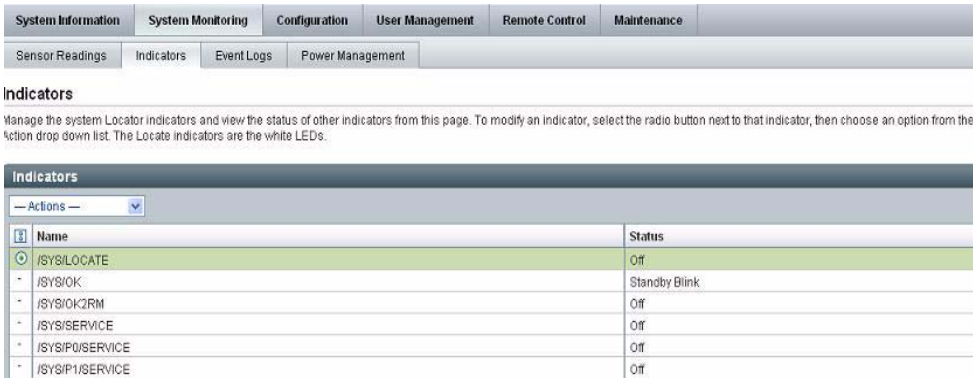
Weitere Informationen zum Anzeigen und Verwalten von System-LEDs in der ILOM-Webbenutzeroberfläche oder -CLI finden Sie unter „Anzeigen und Verwalten von LEDs mithilfe der Webbenutzeroberfläche“ auf Seite 124 und „Anzeigen und Verwalten von LEDs mithilfe der CLI“ auf Seite 125.

- **Vom System zugewiesene Zustände** – Vom System zugewiesene LEDs können *nicht* konfiguriert werden. Diese Typen von System-LEDs bietet schreibgeschützte Werte zum Betriebsstatus einer Komponente. Bei den meisten Serverplattformen sind vom System zugewiesene LEDs *„Wartungsaktion erforderlich“-LEDs* (Service Action Required). Diese Typen von LEDs leuchten normalerweise auf, wenn einer der folgenden Zustände erkannt wird:
  - Versagen bzw. Fehler in einer Systemkomponente wurde erkannt.
  - Hot-Plug-Modul ist zum Entfernen bereit.
  - FRU (Field Replaceable Unit) benötigt Wartung.

## Anzeigen und Verwalten von LEDs mithilfe der Webbenutzeroberfläche

In der ILOM-Webbenutzeroberfläche werden System-LEDs auf der Seite Indicators angezeigt und verwaltet. Diese Seite listet die System-LEDs nach Name und Status auf. System-LEDs, die veränderbare Zustände bieten, werden mit einem Optionsfeld angezeigt. Zum Ändern eines veränderbaren LED-Zustands aktivieren Sie das Optionsfeld und wählen dann einen Zustand im Dropdown-Listenfeld Actions aus.

**ABBILDUNG 7-3** Seite Indicators




Weitere Informationen zum Ermitteln von unmittelbaren Sensormesswerten mithilfe der ILOM-Webbenutzeroberfläche finden Sie unter „Ermitteln von Sensormesswerten mithilfe der Webbenutzeroberfläche“ auf Seite 133.

## Anzeigen und Verwalten von LEDs mithilfe der CLI

In der ILOM-CLI kann auf alle System-LEDs im Namespace `/SYS` oder `/CH` zugegriffen werden. Üblicherweise wird mit dem Befehl `cd` zum System-LED-Ziel navigiert und dann mit dem Befehl `show` die Eigenschaften des Ziels angezeigt. Der Zustand einer System-LED kann mithilfe des Befehls `set` geändert werden. Der Befehl `set` wird nur für System-LEDs unterstützt, die über einen veränderbaren Zustand verfügen. Um zu ermitteln, ob der Zustand einer System-LED veränderbar ist, navigieren Sie mit dem Befehl `cd` zum LED-Ziel und zeigen dann mit dem Befehl `show` die System-LED-Eigenschaften an. Beispiel:

`cd /SYS/`*`LED_Ziel`* `oder cd /CH/`*`LED_Ziel`*
`show`

Der System-LED zugeordnete Ziele, Eigenschaften und Befehle werden angezeigt, beispielsweise:

```
Targets:
Properties:
Type = indicator
Value = Off
Commands:
  cd
  set
  show
```

Wenn der Befehl `set` in der Liste `Commands` aufgeführt wird, ist der Zustand der System-LED veränderbar. Verwenden Sie zum Ändern des Zustands der System-LED folgende Syntax:

`set value=`*`Zustands_name`*

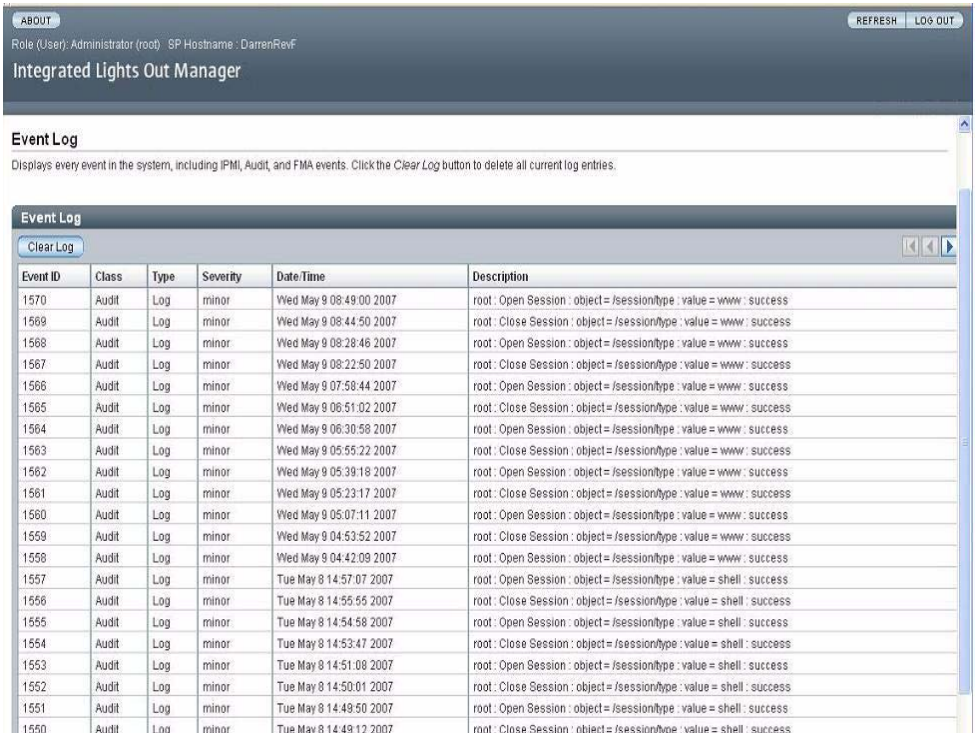
Weitere Informationen zu den auf Ihrem System unterstützten System-LEDs sowie deren Zugriffspfade finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

# ILOM-Ereignisprotokoll

Mithilfe des ILOM-Ereignisprotokolls können Sie Informationen zu allen Ereignissen anzeigen, die im System aufgetreten sind. Ereignisse können unter anderem ILOM-Konfigurationsänderungen, Softwareereignisse, Warnungen, Alarme, Komponentenversagen sowie IPMI-Ereignisse sein. Der Typ der im ILOM-Ereignisprotokoll aufgezeichneten Ereignisse wird von der Serverplattform bestimmt. Spezifische Informationen darüber, welche Ereignisse im ILOM-Ereignisprotokoll aufgezeichnet werden, finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

Das ILOM-Ereignisprotokoll kann in der ILOM-Webbenutzeroberfläche oder in der CLI angezeigt und verwaltet werden. Weitere Information zum Anzeigen und Verwalten des ILOM-Ereignisprotokolls finden Sie unter „Anzeigen und Löschen des ILOM-Ereignisprotokolls mithilfe der Webbenutzeroberfläche“ auf Seite 134 und „Anzeigen und Löschen des ILOM-Ereignisprotokolls mithilfe der CLI“ auf Seite 136.

**ABBILDUNG 7-4** Beispiel für das ILOM-Ereignisprotokoll


ABOUT
REFRESH
LOG OUT
Role (User): Administrator (root) SP Hostname : DarrenRevF
Integrated Lights Out Manager
Event Log
Displays every event in the system, including IPMI, Audit, and FMA events. Click the Clear Log button to delete all current log entries.
Event Log
Clear Log
Event ID | Class | Type | Severity | Date/Time | Description
1570 | Audit | Log | minor | Wed May 9 08:49:00 2007 | root : Open Session : object = /session/type : value = www : success
1569 | Audit | Log | minor | Wed May 9 08:44:50 2007 | root : Close Session : object = /session/type : value = www : success
1568 | Audit | Log | minor | Wed May 9 08:28:46 2007 | root : Open Session : object = /session/type : value = www : success
1567 | Audit | Log | minor | Wed May 9 08:22:50 2007 | root : Close Session : object = /session/type : value = www : success
1566 | Audit | Log | minor | Wed May 9 07:58:44 2007 | root : Open Session : object = /session/type : value = www : success
1565 | Audit | Log | minor | Wed May 9 06:51:02 2007 | root : Close Session : object = /session/type : value = www : success
1564 | Audit | Log | minor | Wed May 9 06:30:58 2007 | root : Open Session : object = /session/type : value = www : success
1563 | Audit | Log | minor | Wed May 9 05:55:22 2007 | root : Close Session : object = /session/type : value = www : success
1562 | Audit | Log | minor | Wed May 9 05:39:18 2007 | root : Open Session : object = /session/type : value = www : success
1561 | Audit | Log | minor | Wed May 9 05:23:17 2007 | root : Close Session : object = /session/type : value = www : success
1560 | Audit | Log | minor | Wed May 9 05:07:11 2007 | root : Open Session : object = /session/type : value = www : success
1559 | Audit | Log | minor | Wed May 9 04:53:52 2007 | root : Close Session : object = /session/type : value = www : success
1558 | Audit | Log | minor | Wed May 9 04:42:09 2007 | root : Open Session : object = /session/type : value = www : success
1557 | Audit | Log | minor | Tue May 8 14:57:07 2007 | root : Open Session : object = /session/type : value = shell : success
1556 | Audit | Log | minor | Tue May 8 14:55:55 2007 | root : Close Session : object = /session/type : value = shell : success
1555 | Audit | Log | minor | Tue May 8 14:54:58 2007 | root : Open Session : object = /session/type : value = shell : success
1554 | Audit | Log | minor | Tue May 8 14:53:47 2007 | root : Close Session : object = /session/type : value = shell : success
1553 | Audit | Log | minor | Tue May 8 14:51:08 2007 | root : Open Session : object = /session/type : value = shell : success
1552 | Audit | Log | minor | Tue May 8 14:50:01 2007 | root : Close Session : object = /session/type : value = shell : success
1551 | Audit | Log | minor | Tue May 8 14:49:50 2007 | root : Open Session : object = /session/type : value = shell : success
1550 | Audit | Log | minor | Tue May 8 14:49:12 2007 | root : Close Session : object = /session/type : value = shell : success

# Ereignisprotokoll-Zeitstempel und ILOM-Zeiteinstellungen

ILOM erfasst Zeitstempel im Ereignisprotokoll auf Grundlage der UTC/GMT-Zeitzone des Hostservers. Beim Anzeigen des Ereignisprotokolls von einem Clientsystem aus, das sich in einer anderen Zeitzone befindet, werden die Zeitstempel jedoch automatisch an die Zeitzone des Clientsystems angepasst. Deshalb kann es vorkommen, dass ein einzelnes Ereignis mit zwei Zeitstempeln im ILOM-Ereignisprotokoll aufgeführt wird.

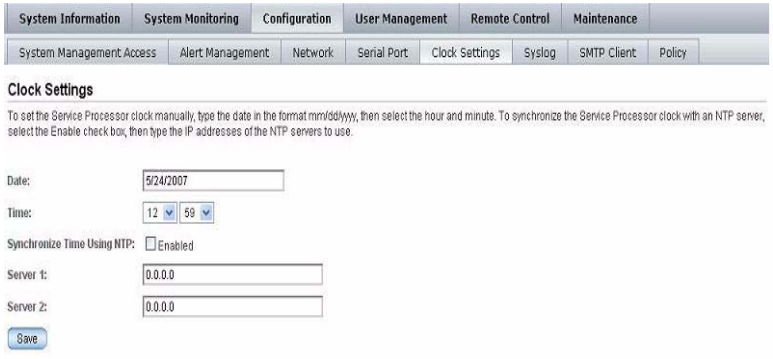
## Unterstützte Zeiteinstellungen

In ILOM können Sie auswählen, ob die ILOM-Uhr manuell auf Grundlage der UTC/GMT-Zeitzone des Hostservers konfiguriert werden soll, oder ob die ILOM-Uhr mit anderen Systemen im Netzwerk synchronisiert werden soll, indem die ILOM-Uhr mit einer NTP-Server-IP-Adresse konfiguriert wird.

## Anzeigen und Festlegen von Zeiteinstellungen mithilfe der Webbenutzeroberfläche

Die ILOM-Zeiteinstellungen können in der ILOM-Webbenutzeroberfläche auf der Seite Configuration --> Clock Settings angezeigt und festgelegt werden.

**ABBILDUNG 7-5** Seite Clock Settings




Weitere Information zum Anzeigen und Festlegen von Zeiteinstellungen in der ILOM-Webbenutzeroberfläche finden Sie unter „Anzeigen und Konfigurieren von Zeiteinstellungen mithilfe der Webbenutzeroberfläche“ auf Seite 138.

## Anzeigen und Festlegen von Zeiteinstellungen mithilfe der CLI

Die ILOM-Zeiteinstellungen können in der ILOM-CLI mithilfe des Befehls `show` angezeigt werden. Auf einigen Serverplattformen können Sie die Zeiteinstellungen beispielsweise durch Angabe des folgenden Pfads anzeigen:

```
show /sp/clock
```

Die ILOM-Zeiteinstellung kann in der CLI mithilfe der folgenden Syntax des Befehls `show` manuell konfiguriert werden:

`set target` *Eigenschaften_name=Wert*

Sie können die ILOM-Zeiteinstellung in der ILOM-CLI auch so konfigurieren, dass sie mit anderen Systemen im Netzwerk synchronisiert wird, indem Sie eine IP-Adresse eines NTP-Servers festlegen. Auf einigen Serverplattformen können Sie beispielsweise den folgenden Pfad eingeben, um die IP-Adresse eines NTP-Servers festzulegen, und im Anschluss die NTP-Synchronisierung aktivieren.

- Beispiel für das Festlegen einer NTP-Server-IP-Adresse:

`set /SP/clients/ntp/server/1 address=`*IP_Adresse*

- Beispiel für das Aktivieren der Synchronisierung:

```
set /SP/clock/usentpserver=enabled
```

Weitere Informationen zum Konfigurieren der ILOM-Zeiteinstellungen in der ILOM-CLI finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

Zusätzlich können Sie die Benutzerdokumentation Ihrer Serverplattform heranziehen, um plattformspezifische Zeitinformationen zu folgenden Themen zu erhalten:

- Die aktuelle Zeit in ILOM bleibt auch nach Neustarts des SP bestehen.
- Die aktuelle Zeit in ILOM kann mit dem Host zum Zeitpunkt des Neustarts des Hosts synchronisiert werden.
- Ein Echtzeituhr-Element (RTC), das die Zeit speichert, ist vorhanden.

# Syslog-Informationen

Syslog ist eine Standardprotokollierungsfunktion, die in zahlreichen Umgebungen verwendet wird. Syslog definiert einen allgemeinen Satz von Leistungsmerkmalen für das Protokollieren von Ereignissen sowie ein Protokoll für die Übermittlung von Ereignissen an einen entfernten Protokollhost. Mithilfe von Syslog können Sie Ereignisse von mehreren ILOM-Instanzen an einem einzigen Ort kombinieren. Der Protokolleintrag enthält alle identischen Informationen, die im jeweiligen lokalen ILOM-Ereignisprotokoll angezeigt werden, einschließlich Klasse, Typ, Schweregrad und Beschreibung. Informationen zum Konfigurieren von ILOM

zum Senden von Syslog an eine oder zwei IP-Adressen finden Sie unter „Konfigurieren von IP-Adressen von entfernten Syslog-Empfängern mithilfe der Webbenutzeroberfläche“ auf Seite 139 und „Konfigurieren von IP-Adressen von entfernten Syslog-Empfängern mithilfe der CLI“ auf Seite 140.

# Fehlerverwaltung

Die meisten Serverplattformen beinhalten die Sofwarefehlerverwaltungs-Funktion von ILOM. Mithilfe dieses Leistungsmerkmals kann der Zustand der Systemhardware proaktiv überwacht und bei Auftreten von Hardarefehlern eine Diagnose durchgeführt werden. Zusätzlich zur Überwachung der Systemhardware überwacht die Fehlerverwaltungssoftware Umgebungsbedingungen und meldet, wenn die Umgebung des Systems außerhalb akzeptabler Parameterwerte liegt. Verschiedene Sensoren an den Systemkomponenten werden kontinuierlich überwacht. Sobald ein Problem erkannt wird, führt die Fehlerverwaltungssoftware folgende Aktionen automatisch durch:

- Aktivieren (Aufleuchten) der „Wartungsaktion erforderlich“-LED (Server Action Required) an der fehlerhaften Komponente.
- Aktualisieren der ILOM-Verwaltungsoberflächen mit der Anzeige des Fehlerzustands.
- Aufzeichnen von Informationen zu dem Fehler im ILOM-Ereignisprotokoll.

Der Status von fehlerhaften Komponenten kann über die ILOM-Webbenutzeroberfläche oder die ILOM-CLI angezeigt werden. Weitere Informationen zu diesem Thema finden Sie unter:

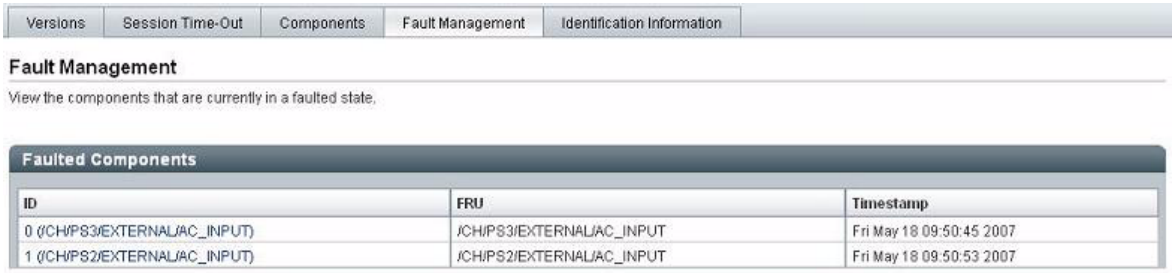
- „Anzeigen des Fehlerstatus mithilfe der Webbenutzeroberfläche“ auf Seite 130
- „Anzeigen des Fehlerstatus mithilfe der CLI“ auf Seite 131.

Die Typen von Systemkomponenten und Umgebungsbedingungen, die von der Fehlerverwaltungssoftware überwacht werden, sind von der jeweiligen Serverplattform abhängig. Ausführliche Informationen darüber, welche Komponenten von der Fehlerverwaltungssoftware überwacht werden, finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

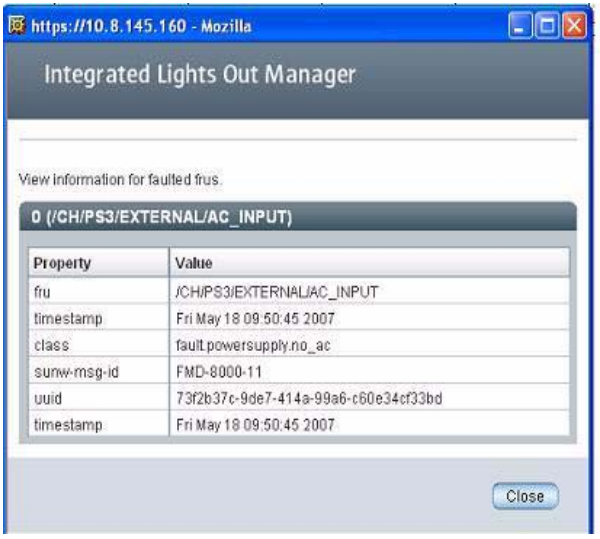
## Anzeigen des Fehlerstatus mithilfe der Webbenutzeroberfläche

In der ILOM-Webbenutzeroberfläche können Sie die Systemkomponenten, die sich aktuell in einem Fehlerzustand befinden, auf der Seite Fault Management anzeigen.

**ABBILDUNG 7-6** Beispiel für die Seite Fault Management




Auf der Seite Fault Management werden fehlerhafte Komponenten nach ID, FRU und Timestamp (Zeitstempel) aufgelistet. Sie können auf zusätzliche Informationen zu der fehlerhaften Komponente zugreifen, indem Sie auf deren ID klicken. Wenn Sie beispielsweise auf die fehlerhafte Komponenten-ID `0(CH/PS3/EXTERNAL/AC_INPUT)` klicken, wird folgendes Dialogfeld mit zusätzlichen Detailinformationen zu der fehlerhaften Komponente angezeigt.



Alternativ können Sie in der ILOM-Webbenutzeroberfläche auf der Seite Component Management den Fehlerstatus einer Komponente identifizieren.

**ABBILDUNG 7-7** Seite Component Management – Fault Status

Component Management Status

| Component Name | Type | Ready to Remove Status | Fault Status |
|---|---|---|---|
| / | Container | - | OK |
| /SYS | Host System | - | OK |
| /SYS/BIOS | BIOS | - | - |
| /SYS/P0 | Host Processor | - | OK |
| /SYS/P0/D0 | DIMM | - | OK |
| /SYS/P0/D1 | DIMM | - | OK |
| /SYS/P1 | Host Processor | - | OK |
| /SYS/P2 | Host Processor | - | OK |
| /SYS/P3 | Host Processor | - | OK |
| /SYS/HDD0 | Hard Disk | - | OK |

Weitere Informationen zu den ILOM-Fehlerverwaltungsfunktionen, die auf Ihrem System verfügbar sind, finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

## Anzeigen des Fehlerstatus mithilfe der CLI

Der Fehlerstatus von Komponenten kann in der ILOM-CLI mithilfe des Befehls `show` angezeigt werden. In Abhängigkeit von der Serverplattform können Sie beispielsweise einen der folgenden Pfade angeben:

```
show /SP/faultmgmt
show /CH/faultmgmt
```

Weitere Informationen zu den ILOM-Fehlerverwaltungsfunktionen, die auf Ihrem System verfügbar sind, finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

# Überwachen von Systemsensoren, LEDs und des ILOM-Ereignisprotokolls

Informationen zum Überwachen von Systemsensoren, System-LEDs und Ereignissen im ILOM-Ereignisprotokoll finden Sie in den folgenden Verfahren.


- „Ermitteln des Zustands von LEDs mithilfe der Webbenutzeroberfläche“ auf Seite 132
- „Ermitteln von Sensormesswerten mithilfe der Webbenutzeroberfläche“ auf Seite 133
- „Anzeigen und Löschen des ILOM-Ereignisprotokolls mithilfe der Webbenutzeroberfläche“ auf Seite 134
- „Anzeigen und Löschen des ILOM-Ereignisprotokolls mithilfe der CLI“ auf Seite 136
- „Anzeigen und Konfigurieren von Zeiteinstellungen mithilfe der Webbenutzeroberfläche“ auf Seite 138
- „Konfigurieren von IP-Adressen von entfernten Syslog-Empfängern mithilfe der Webbenutzeroberfläche“ auf Seite 139
- „Konfigurieren von IP-Adressen von entfernten Syslog-Empfängern mithilfe der CLI“ auf Seite 140


## ▼ Ermitteln des Zustands von LEDs mithilfe der Webbenutzeroberfläche

Führen Sie diese Schritte durch, um den Zustand von System-LEDs in der ILOM-Webbenutzeroberfläche zu ermitteln:

1. **Öffnen Sie einen Webbrowser, und geben Sie die IP-Adresse des Server-SP oder CMM ein.**

   Die Anmeldeseite der ILOM-Webbenutzeroberfläche wird angezeigt.

2. **Geben Sie auf der Seite ILOM Login einen Benutzernamen mit Passwort ein, und klicken Sie auf OK.**

   Die ILOM-Webbenutzeroberfläche wird angezeigt.

3. **Wählen Sie auf der Webbenutzeroberflächenseite System Monitoring --> Indicators.**

   Die Seite Indicators wird angezeigt.

---

**Hinweis –** Wenn der Server ausgeschaltet ist, werden zahlreiche LEDs als „no reading“ (kein Messwert) angezeigt.

---

4. **Führen Sie auf der Seite Indicators Folgendes aus:**

   a. **Suchen Sie den Namen der anzuzeigenden LED.**

   b. **Um den Zustand einer LED umzuschalten (ein/aus), klicken Sie zuerst auf das Optionsfeld, das der umzuschaltenden LED zugeordnet ist, und dann auf das Dropdown-Listenfeld Actions, in dem Sie einen der Einträge Turn LED Off oder Set LED to Fast Blink auswählen.**

      Daraufhin werden Si in einem Dialogfeld zum Bestätigen der Änderung aufgefordert.

   c. **Klicken Sie hierzu auf OK.**

## ▼ Ermitteln von Sensormesswerten mithilfe der Webbenutzeroberfläche

Führen Sie diese Schritte durch, um Sensormesswerte in der ILOM-Webbenutzeroberfläche zu ermitteln:

1. **Öffnen Sie einen Webbrowser, und geben Sie die IP-Adresse des Server-SP oder CMM ein.**

   Die Anmeldeseite der ILOM-Webbenutzeroberfläche wird angezeigt.

2. **Geben Sie auf der Seite ILOM Login einen Benutzernamen mit Passwort ein, und klicken Sie auf OK.**

   Die ILOM-Webbenutzeroberfläche wird angezeigt.

3. **Klicken Sie auf der Webbenutzeroberflächenseite auf System Monitoring --> Sensors Readings.**

   Die Seite Sensor Readings wird angezeigt.

---

**Hinweis –** Wenn der Server ausgeschaltet ist, werden zahlreiche Komponenten als „no reading“ (kein Messwert) angezeigt.

---

4. **Führen Sie auf der Seite Sensor Readings Folgendes aus:**

   a. **Suchen Sie den Namen des anzuzeigenden Sensors.**

   b. **Klicken Sie auf den Namen des Sensors, um die ihm zugeordneten Eigenschaftenwerte anzuzeigen.**

Spezifische Detailinformationen zu den Typen von diskreten Sensorzielen, die verfügbar sind, sowie deren Zugriffspfade finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

## ▼ Anzeigen und Löschen des ILOM-Ereignisprotokolls mithilfe der Webbenutzeroberfläche

Führen Sie diese Schritte durch, um Ereignisse im ILOM-Ereignisprotokoll mithilfe der ILOM-Webbenutzeroberfläche anzuzeigen oder zu löschen:

1. **Öffnen Sie einen Webbrowser, und geben Sie die IP-Adresse des Server-SP oder CMM ein.**

   Die Anmeldeseite der ILOM-Webbenutzeroberfläche wird angezeigt.

2. **Geben Sie auf der Seite ILOM Login einen Benutzernamen mit Passwort ein, und klicken Sie auf OK.**

   Die ILOM-Webbenutzeroberfläche wird angezeigt.

3. **Wählen Sie auf der Webbenutzeroberflächenseite System Monitoring --> Event Logs.**

   Die Seite Event Log wird angezeigt.

4. **Auf der Seite Event Log können Sie folgende Aktionen ausführen:**

   - **Durchblättern von Einträgen** – Mithilfe der Steuerelemente für die Seitennavigation am oberen und unteren Rand der Tabelle können Sie sich innerhalb der in der Tabelle verfügbaren Daten vor- und zurückbewegen.

     Beachten Sie, dass das Auswählen einer größeren Anzahl von Einträgen zu einer langsameren Reaktion der Webbenutzeroberfläche führen kann als bei einer kleineren Anzahl von Einträgen.

   - **Anzeigen der Einträge mithilfe eines Bildlaufs durch die Liste** – Die folgende Tabelle bietet Beschreibungen zu jeder Spalte, die im Protokoll vorkommt.

| Spaltenbezeichnung | Beschreibung |
|---|---|
| Event ID | Die Nummer des Ereignisses in fortlaufender Reihenfolge, beginnend bei 1. |
| Class/Type | • Audit/Log – Befehle, die zu einer Konfigurationsänderung führen. Die Beschreibung umfasst den Benutzer, den Befehl, die Befehlsparameter und ob der Vorgang erfolgreich/fehlerhaft war.<br>• IPMI/Log – Jedes Ereignis, das im IPMI-SEL erfasst wird, wird ebenfalls im Verwaltungsprotokoll erfasst.<br>• Chassis/State – Für Änderungen am Bestand und allgemeine Systemzustandänderungen.<br>• Chassis/Action – Kategorie für Herunterfahren-Ereignisse für das Servermodul/-gehäuse, das Einsetzen/Entfernen einer FRU im laufenden Betrieb und bei Drücken des Schalters Reset Parameters.<br>• FMA/Fault – Für Fehler in der Fehlerverwaltungsarchitektur (Fault Management Architecture, FMA). In der Beschreibung werden die Zeit, zu der der Fehler von der FMA erkannt wurde, sowie die vermutlich beteiligte Komponente angegeben.<br>• FMA/Repair – Für FMA-Reparaturen. In der Beschreibung wird die Komponente angegeben. |
| Severity | Critical (Kritisch), Major (Schwer wiegend) oder Minor (Geringfügig). |
| Date/Time | Tag und Uhrzeit, zu denen das Ereignis aufgetreten ist. Wenn das Festlegen der ILOM-Zeit durch einen NTP-Server (Network Time Protocol) aktiviert ist, verwendet die ILOM-Uhr die koordinierte Weltzeit (Universal Coordinated Time, UTC). |
| Beschreibung | Eine Beschreibung des Ereignisses. |

- **Löschen des Ereignisprotokolls** – Zum Löschen des Ereignisprotokolls klicken Sie auf die Schaltfläche Clear Event Log. Ein Bestätigungsdialogfeld wird angezeigt. Klicken Sie darin auf OK, um die Einträge zu löschen.

**Hinweis –** Im ILOM-Ereignisprotokoll werden zahlreiche Typen von Ereignissen, einschließlich Kopien von IPMI-Einträgen, gesammelt. Durch das Löschen des ILOM-Ereignisprotokolls werden alle im Protokoll enthaltenen Einträge, einschließlich der IPMI-Einträge, gelöscht. Die direkt in einem IPMI-Protokoll abgelegten Originaleinträge werden aber durch das Löschen der ILOM-Ereignisprotokolleinträge nicht gelöscht.

## ▼ Anzeigen und Löschen des ILOM-Ereignisprotokolls mithilfe der CLI

Führen Sie diese Schritte durch, um Ereignisse im Systemereignisprotokoll mithilfe der ILOM-CLI anzuzeigen oder zu löschen:

1. **Stellen Sie eine lokale serielle Konsolenverbindung oder eine SSH-Verbindung mit dem Server-SP oder CMM her.**

   - **Lokale serielle Konsolenverbindung**

   **Schließen Sie eine serielle Konsole am seriellen Anschluss des Servers oder des CMM an.**

   Weitere Informationen finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

   oder

   - **Entfernte SSH-Verbindung (Secure Shell)**

   **Stellen Sie eine SSH-Verbindung mit dem Server-SP oder CMM her.**

   Stellen Sie von dem entfernten Client aus eine sichere Verbindung als root-Benutzer mit dem Server-SP oder dem aktiven CMM her.

   Sie können beispielsweise eine sichere Verbindung von einem entfernten SSH-Client aus mit dem Server-SP herstellen, indem Sie Folgendes eingeben:

   **`ssh -l root`** *server_ip_adresse*

   `Passwort:` **`changeme`**

   Die Standard-Befehlseingabeaufforderung wird angezeigt (->).

2. **Geben Sie einen der folgenden Befehlspfade ein, um das Arbeitsverzeichnis festzulegen:**

   - Bei einem Rack-System-Server-SP: **`cd /SP/logs/event`**
   - Bei einem Blade-Server-SP im Gehäuse: **`cd /CH/BL`*n*`/SP/logs/event`**
   - Bei einem CMM: **`cd /CMM/logs/event`**

3. **Geben Sie folgenden Befehlspfad ein, um die Ereignisprotokollliste anzuzeigen.**

   **`show list`**

   Der Inhalt des Ereignisprotokolls wird angezeigt. Beispiel:

```
ID     Date/Time                Class     Type      Severity
-----  -----------------------  --------  --------  --------
1522   Sun Jul 30 01:11:36 2006  Audit     Log       minor
       root : Close Session : object = /session/type : value = www : success
1521   Sun Jul 30 01:05:34 2006  Audit     Log       minor
       root : Close Session : session ID = 1307912184 : success
```

.

4. **Im Ereignisprotokoll können Sie folgende Aufgaben ausführen:**

   - **Anzeigen der Einträge mithilfe eines Bildlaufs nach unten in der Liste** – Drücken Sie eine beliebige Taste außer „q“. Die folgende Tabelle bietet Beschreibungen zu jeder Spalte, die im Protokoll vorkommt.

| Spaltenbezeichnung | Beschreibung |
|---|---|
| Event ID | Die Nummer des Ereignisses in fortlaufender Reihenfolge, beginnend bei 1. |
| Class/Type | • Audit/Log – Befehle, die zu einer Konfigurationsänderung führen. Die Beschreibung umfasst den Benutzer, den Befehl, die Befehlsparameter und ob der Vorgang erfolgreich/fehlerhaft war.<br>• IPMI/Log – Jedes Ereignis, das im IPMI-SEL erfasst wird, wird ebenfalls im Verwaltungsprotokoll erfasst.<br>• Chassis/State – Für Änderungen am Bestand und allgemeine Systemzustandänderungen.<br>• Chassis/Action – Kategorie für Herunterfahren-Ereignisse für das Servermodul/-gehäuse, das Einsetzen/Entfernen einer FRU im laufenden Betrieb und bei Drücken des Schalters Reset Parameters.<br>• FMA/Fault – Für Fehler in der Fehlerverwaltungsarchitektur (Fault Management Architecture, FMA). In der Beschreibung werden die Zeit, zu der der Fehler von der FMA erkannt wurde, sowie die vermutlich beteiligte Komponente angegeben.<br>• FMA/Repair – Für FMA-Reparaturen. In der Beschreibung wird die Komponente angegeben. |
| Severity | Critical (Kritisch), Major (Schwer wiegend) oder Minor (Geringfügig). |
| Date/Time | Tag und Uhrzeit, zu denen das Ereignis aufgetreten ist. Wenn das Festlegen der ILOM-Zeit durch einen NTP-Server (Network Time Protocol) aktiviert ist, verwendet die ILOM-Uhr die koordinierte Weltzeit (Universal Coordinated Time, UTC). |
| Beschreibung | Eine Beschreibung des Ereignisses. |

   - **Beenden des Ereignisprotokolls (Beenden der Protokollanzeige)** – Drücken Sie die Taste „q“.
   - **Löschen von Einträgen im Ereignisprotokoll** – Führen Sie folgende Schritte durch:

   **a. Geben Sie Folgendes ein: `set clear=true`**

   Eine Bestätigungsmeldung wird angezeigt.

   **b. Nehmen Sie eine der folgenden Eingaben vor:**

   - Zum Löschen der Einträge geben Sie Folgendes ein: **`y`**.
   - Zum Abbrechen des Protokolllöschvorgangs geben Sie Folgendes ein: **`n`**.

**Hinweis –** Im ILOM-Ereignisprotokoll werden zahlreiche Typen von Ereignissen, einschließlich Kopien von IPMI-Einträgen, gesammelt. Durch das Löschen des ILOM-Ereignisprotokolls werden alle im Protokoll enthaltenen Einträge, einschließlich der IPMI-Einträge, gelöscht. Die direkt in einem IPMI-Protokoll abgelegten Originaleinträge werden aber durch das Löschen der ILOM-Ereignisprotokolleinträge nicht gelöscht.

## ▼ Anzeigen und Konfigurieren von Zeiteinstellungen mithilfe der Webbenutzeroberfläche

Um dieses Verfahren durchführen zu können, benötigen Sie die IP-Adresse des NTP-Servers.

1. **Öffnen Sie einen Webbrowser, und geben Sie die IP-Adresse des Server-SP oder CMM ein.**

   Die Anmeldeseite der ILOM-Webbenutzeroberfläche wird angezeigt.

2. **Geben Sie auf der Seite ILOM Login einen Benutzernamen mit Passwort ein, und klicken Sie auf OK.**

   Die ILOM-Webbenutzeroberfläche wird angezeigt.

3. **Klicken Sie auf der Webbenutzeroberflächenseite auf Configuration --> Clock Settings.**

   Die Seite Clock Settings wird angezeigt.

4. **Führen Sie auf der Seite Clock Settings eine der folgenden Aktionen aus:**
   - Anzeigen der vorhandenen Einstellungen.
   - Manuelles Konfigurieren von Datum und Uhrzeit des Hostserver-SP:

     a. **Geben Sie im Textfeld Date das Datum im Format „MM/TT/JJ“ ein.**

     b. **Legen Sie in den Zeit-Dropdown-Listenfeldern die Stunden und Minuten fest.**
   - Konfigurieren einer IP-Adresse eines NTP-Servers und Aktivieren der Synchronisierung.

     a. **Aktivieren Sie das Kontrollkästchen Enabled neben Synchronize Time Using NTP.**

     b. **Geben Sie in das Textfeld Server 1 die IP-Adresse des primären NTP-Servers ein, der verwendet werden soll.**

     c. **(Optional) Geben Sie in das Textfeld Server 2 die IP-Adresse des sekundären NTP-Servers ein, der verwendet werden soll.**

5. **Klicken Sie auf Save, um die Änderungen zu übernehmen.**

## ▼ Konfigurieren von IP-Adressen von entfernten Syslog-Empfängern mithilfe der Webbenutzeroberfläche

Führen Sie diese Schritte durch, um in ILOM mithilfe der Webbenutzeroberfläche eine IP-Adresse für einen entfernten Syslog-Empfänger zu konfigurieren:

1. **Öffnen Sie einen Webbrowser, und geben Sie die IP-Adresse des Server-SP oder CMM ein.**

   Die Anmeldeseite der ILOM-Webbenutzeroberfläche wird angezeigt.

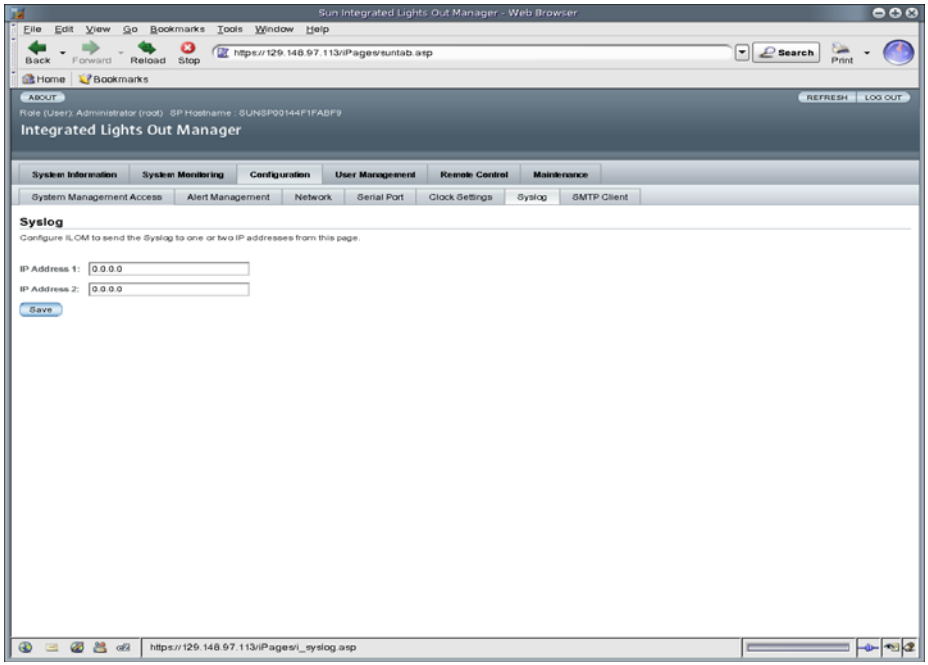
2. **Geben Sie auf der Seite ILOM Login einen Benutzernamen mit Passwort ein, und klicken Sie auf OK.**

   Die ILOM-Webbenutzeroberfläche wird angezeigt.

3. **Wählen Sie in der ILOM-Webbenutzeroberfläche Configuration --> Syslog.**

   Die Seite Syslog wird angezeigt.

**ABBILDUNG 7-8** Seite Syslog




4. **Geben Sie in den Feldern IP Address 1 und IP Address 2 die IP-Adressen für die zwei Standorte ein, an die Syslog-Daten gesendet werden sollen.**

5. **Klicken Sie auf Save, um die neuen Einstellungen zu übernehmen.**

## ▼ Konfigurieren von IP-Adressen von entfernten Syslog-Empfängern mithilfe der CLI

Führen Sie diese Schritte durch, um mithilfe der CLI eine IP-Adresse für einen entfernten Syslog-Empfänger zu konfigurieren:

1. **Stellen Sie eine lokale serielle Konsolenverbindung oder eine SSH-Verbindung mit dem Server-SP oder CMM her.**

   - **Lokale serielle Konsolenverbindung**

     **Schließen Sie eine serielle Konsole am seriellen Anschluss des Servers oder des CMM an.**

     Weitere Informationen finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

   oder

   - **Entfernte SSH-Verbindung (Secure Shell)**

     **Stellen Sie eine SSH-Verbindung mit dem Server-SP oder CMM her.**

     Stellen Sie von dem entfernten Client aus eine sichere Verbindung als root-Benutzer mit dem Server-SP oder dem aktiven CMM her.

     Sie können beispielsweise eine sichere Verbindung von einem entfernten SSH-Client aus mit dem Server-SP herstellen, indem Sie Folgendes eingeben:

     **`ssh -l root`** *server_ip_adresse*

     `Passwort:` **`changeme`**

     Die Standard-Befehlseingabeaufforderung wird angezeigt (->).

2. **Geben Sie einen der folgenden Befehlspfade ein, um das Arbeitsverzeichnis festzulegen:**

   - Bei einem Rack-System-Server-SP: **`cd /SP/clients/syslog`**
   - Bei einem Blade-Server-SP im Gehäuse: **`cd /CH/BL`*n*`/SP/clients/syslog`**
   - Bei einem CMM: **`cd /CMM/clients/syslog`**

3. **Geben Sie den Befehl `show` ein, um die Syslog-Eigenschaften anzuzeigen.**

   Die Eigenschaften werden angezeigt. Beim ersten Zugriff auf die Syslog-Eigenschaften auf einem SP wird ungefähr Folgendes angezeigt:

```
/SP/clients/syslog
Targets:
Properties:
   destination_ip1 = 0.0.0.0
   destination_ip2 = 0.0.0.0
Commands:
   cd
   set
   show
```

4. **Geben Sie mithilfe des Befehls `set` eine Ziel-IP-Adresse für IP 1 (und ggf. für IP 2) an.**

   Um beispielsweise ein IP-Ziel auf die IP-Adresse 11.222.33.4 festzulegen, würden Sie Folgendes eingeben:

   ```
   set destination_ip1=111.222.33.4
   ```

5. **Drücken Sie die Eingabetaste, um die Einstellung zu übernehmen.**

   Die Ergebnisse der der IP-Adresseneinstellung werden angezeigt.
   Würde beispielsweise die Ziel-IP-Adresse auf 111.222.33.4 festgelegt, würde Folgendes angezeigt:

   ```
   Set 'destination_ip1' to '111.222.33.4'
   ```

# Informationen zur Alarmverwaltung

Alarme bieten Vorabwarnungen bei möglichen Systemfehlern. Jede Serverplattformen ist mit einer Anzahl von Sensoren ausgestattet, die die Spannung, Temperaturen und andere betriebsbezogene Attribute des Systems messen. ILOM ruft diese Sensoren automatisch ab und erfasst alle Ereignisse, die einen Schwellenwert überschreiten, in einem ILOM-Ereignisprotokoll, und erzeugt Alarmmeldungen, die an mindestens ein individuell festgelegtes Alarmziel gesendet werden.

**Achtung –** ILOM markiert alle Ereignisse bzw. Aktionen mit LocalTime=GMT (oder UTC). In Browserclients werden diese Ereignisse in lokaler Zeit (LocalTime) angezeigt. Hierdurch kann es zu merklichen Abweichungen innerhalb des Ereignisprotokolls kommen. Bei Auftreten eines Ereignisses in ILOM wird dieses im Ereignisprotokoll mit koordinierter Weltzeit (UTC), in einem Client aber mit lokaler Zeit angezeigt. Weitere Informationen zu ILOM-Zeitstempeln und -Zeiteinstellungen finden Sie unter „Ereignisprotokoll-Zeitstempel und ILOM-Zeiteinstellungen“ auf Seite 127.

## Konfiguration von Alarmregeln

In ILOM können bis zu 15 Alarmregeln mithilfe der ILOM-Webbenutzeroberfläche oder der -CLI konfiguriert werden. Für jede in ILOM konfigurierte Alarmregel müssen in Abhängigkeit vom Alarmtyp mindestens drei Alarmeigenschaften definiert werden.

Der *Alarmtyp* definiert das Meldungsformat sowie die Methode zum Senden und Empfangen einer Alarmmeldung. ILOM unterstützt die folgenden drei Alarmtypen:

- IPMI PET-Alarme
- SNMP-Trap-Alarme
- E-Mail-Benachrichtigungsalarme

Alle drei Alarmtypen werden von allen Serverplattformen unterstützt, mit Ausnahme des Chassis Monitoring Module (CMM). Das Chassis Monitoring Module unterstützt SNMP-Trap-Alarme und E-Mail-Benachrichtigungsalarme, aber zurzeit keine IPMI PET-Alarme.

Eine kurze Diskussion der einzelnen Alarmtypen sowie der anderen Eigenschaften, mit deren Hilfe eine Alarmregel definiert werden kann, finden Sie im folgenden Abschnitt unter „Definitionen von Alarmregeleigenschaften“ auf Seite 142.

## Definitionen von Alarmregeleigenschaften

ILOM bietet bis zu fünf Eigenschaftenwerte zum Definieren einer Alarmregel, die im Folgenden aufgeführt werden:

- Alert Type
- Alert Level
- Alert Destination
- SNMP Version (*Nur SNMP-Trap-Alarme*)
- SNMP Community Name oder User Name (*Nur SNMP-Trap-Alarme*)

Weitere Informationen zu den einzelnen Eigenschaftenwerten finden Sie in TABELLE 7-1.

**TABELLE 7-1** Eigenschaften zum Definieren von Alarmregeln

| Name der Eigenschaft | Anforderung | Beschreibung |
|---|---|---|
| Alert Type | Obligatorisch | Die Eigenschaft Alert Type (Alarmtyp) gibt das Meldungsformat und die Zustellungsmethode an, die von ILOM beim Erstellen und Senden der Alarmmeldung verwendet werden. Sie können einen der folgenden Alarmtypen konfigurieren:<br>• **IPMI PET-Alarme**. IPMI PET-Alarme (Platform Event Trap, Plattformereignis-Trap) werden auf allen Serverplattformen und Modulen unterstützt, mit Ausnahme des Chassis Monitoring Module (CMM).<br>Für jeden in ILOM konfigurierten IPMI PET-Alarm müssen Sie eine IP-Adresse für ein Alarmziel sowie eine von vier unterstützten Alarmstufen angeben. Beachten Sie, dass das angegebene Alarmziel das Empfangen von IPMI PET-Meldungen unterstützen muss. Unterstützt das Alarmziel den Empfang von IPMI PET-Meldungen nicht, kann der Alarmempfänger die Alarmmeldung nicht dekodieren. |

**TABELLE 7-1** Eigenschaften zum Definieren von Alarmregeln *(Fortsetzung)*

| Name der Eigenschaft | Anforderung | Beschreibung |
|---|---|---|
| | | • **SNMP-Trap-Alarme**. ILOM unterstützt die Erzeugung von SNMP-Trap-Alarmen und das Versenden an ein individuell angegebenes IP-Ziel. Alle angegebenen Ziele müssen das Empfangen von SNMP-Trap-Meldungen unterstützen.<br>Beachten Sie, dass SNMP-Trap-Alarme von Rack-System-Servern und von Blade-Servermodulen unterstützt werden.<br>• **E-Mail-Benachrichtigungsalarme**. ILOM unterstützt die Erzeugung von E-Mail-Benachrichtigungsalarmen und das Versenden an eine individuell angegebene E-Mail-Adresse. Damit der ILOM-Client E-Mail-Benachrichtigungsalarme erzeugen kann, müssen Sie in ILOM zuerst den Namen des ausgehenden SMTP-E-Mail-Servers konfigurieren, von dem die E-Mail-Alarmbenachrichtigungen gesendet werden sollen. Weitere Informationen zu diesem Thema finden Sie unter „Aktivieren eines SMTP-Clients mithilfe der Webbenutzeroberfläche“ auf Seite 156. |
| Alert Destination | Obligatorisch | Die Eigenschaft Alert Destination (Alarmziel) gibt an, wohin die Alarmmeldung gesendet werden soll. Der Alarmtyp bestimmt, welches Ziel für das Senden von Alarmmeldungen gewählt werden kann. Bei IPMI PET- und SNMP-Trap-Alarmen muss beispielsweise das Ziel eine IP-Adresse sein. Für E-Mail-Benachrichtigungsalarme muss dagegen eine E-Mail-Adresse angegeben werden.<br>Wenn nicht das erforderliche Format für ein Alarmziel eingegeben wird, meldet ILOM einen Fehler. |
| Alert Level | Obligatorisch | Alarmstufen fungieren als Filtermechanismus, um sicherzustellen, dass Alarmempfänger nur die Alarmmeldungen empfangen, an deren Erhalt diese primär interessiert sind. Bei jeder Definition einer Alarmregel in ILOM muss eine Alarmstufe angegeben werden.<br>Die Alarmstufe bestimmt, bei welchen Ereignissen ein Alarm erzeugt wird. Der Alarm der niedrigsten Stufe erzeugt Alarme für diese Stufe sowie für alle höheren Alarmstufen.<br>ILOM stellt die folgenden Alarmstufen bereit, wobei Minor (Geringfügig) die niedrigste ist:<br>• **Minor**. Bei dieser Alarmstufe werden Alarme für Informationsereignisse, nicht kritische obere und untere Schwellenwertereignisse, kritische obere und untere Schwellenwertereignisse sowie nicht wiederherstellbare obere und untere Schwellenwertereignisse erzeugt.<br>• **Major.** Bei dieser Alarmstufe werden Alarme für nicht kritische obere und untere Schwellenwertereignisse, kritische obere und untere Schwellenwertereignisse sowie nicht wiederherstellbare obere und untere Schwellenwertereignisse erzeugt. |

**TABELLE 7-1** Eigenschaften zum Definieren von Alarmregeln *(Fortsetzung)*

| Name der Eigenschaft | Anforderung | Beschreibung |
|---|---|---|
| | | • **Critical**. Bei dieser Alarmstufe werden Alarme für kritische obere und untere Schwellenwertereignisse sowie nicht wiederherstellbare obere und untere Schwellenwertereignisse erzeugt.<br>• **Down**. Bei dieser Alarmstufe werden nur Alarme für nicht wiederherstellbare obere und untere Schwellenwertereignisse erzeugt.<br>• **Disabled**. Deaktiviert den Alarm. ILOM erzeugt dann keine Alarmmeldung.<br>Alle Alarmstufen aktivieren das Senden eines Alarms mit Ausnahme von *Disabled*.<br>**Wichtig.** ILOM unterstützt Alarmstufenfilterung für alle IPMI-Traps und E-Mail-Benachrichtigungs-Traps. ILOM unterstützt keine Alarmstunfenfilterung für SNMP-Traps. Zum Aktivieren des Sendens einer SNMP-Trap (aber nicht zum Filtern der SNMP-Trap nach Alarmstufe) können Sie unter den folgenden Optionen auswählen: *minor, major, critical* oder *down*. Zum Deaktivieren des Sendens einer SNMP-Trap müssen Sie die Option *disabled* wählen. |
| SNMP Version | Optional | Mithilfe der Eigenschaft SNMP Version können Sie die Version einer SNMP-Trap angeben, die gesendet wird. Sie können zwischen Folgendem auswählen: 1, 2c oder 3.<br>Dieser Eigenschaftenwert gilt nur für SNMP-Trap-Alarme. |
| SNMP Community Name oder User Name | Optional | Mithilfe der Eigenschaften SNMP Community Name bzw. User Name können Sie die Community-Zeichenfolge oder den SNMP v3-Benutzernamen angeben, die/der in dem SNMP-Trap-Alarm verwendet wird.<br>• Bei SNMP v1- oder v2c-Traps können Sie entscheiden, ob ein „Community Name“-Wert für einen SNMP-Alarm angegeben wird.<br>• Bei SNMP v3-Traps können Sie entscheiden, ob ein „Community User“-Wert für einen SNMP-Alarm angegeben wird.<br>**Wichtig**. Bei Angabe eines SNMP v3-Benutzernamenwerts muss dieser Benutzer in ILOM als SNMP-Benutzer definiert werden. Wird dieser Benutzer nicht als SNMP-Benutzer definiert, kann der Trap-Empfänger den SNMP-Trap-Alarm nicht dekodieren. Weitere Informationen zum Definieren eines SNMP-Benutzers in ILOM finden Sie in Kapitel 10. |

| SMTP-Einstellung | Beschreibung |
|---|---|
| SMTP State | Aktivieren Sie das Kontrollkästchen, um diesen Zustand zu aktivieren. |
| SMTP Server IP | Geben Sie die IP-Adresse des ausgehenden SMTP-E-Mail-Servers ein, von dem die E-Mail-Benachrichtigungen verarbeitet werden sollen. |
| SMTP Port | Geben Sie die Anschlussnummer des ausgehenden SMTP-E-Mail-Servers ein. |

Weitere Information zum Verwalten und Erstellen von Alarmregelkonfigurationen in ILOM finden Sie in den folgenden Abschnitten:

- „Verwalten von Alarmregelkonfigurationen mithilfe der ILOM-Webbenutzeroberfläche“ auf Seite 145.

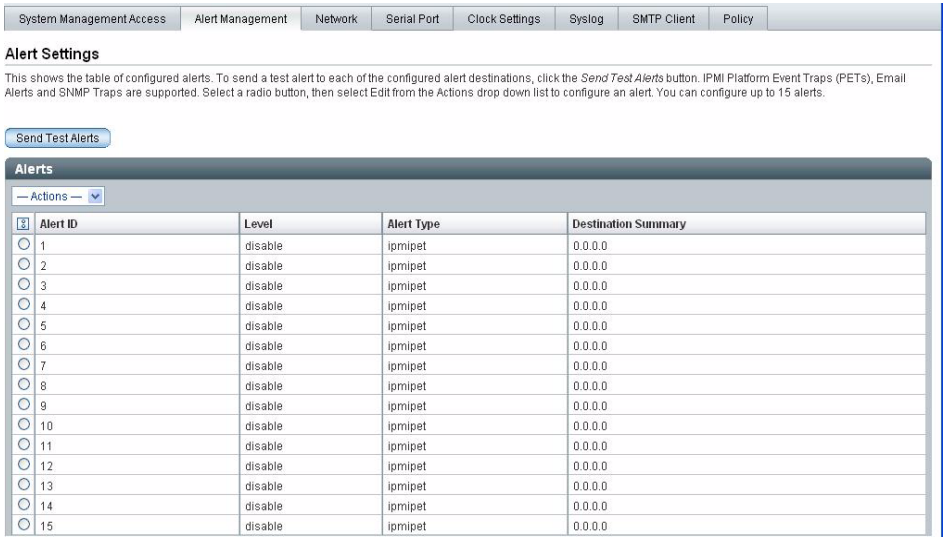
- „Verwalten von Alarmregelkonfigurationen mithilfe der ILOM-CLI“ auf Seite 149.
- „Konfigurieren eines SMTP-Clients für E-Mail-Benachrichtigungsalarme“ auf Seite 155.

# Verwalten von Alarmregelkonfigurationen mithilfe der ILOM-Webbenutzeroberfläche

Alle Alarmregelkonfigurationen können in ILOM auf der Webbenutzeroberflächenseite Alert Settings aktiviert, geändert und deaktiviert werden. Alle 15 auf dieser Seite dargestellten Alarmregelkonfigurationen sind standardmäßig deaktiviert. In dem Dropdown-Listenfeld Actions auf der Seite können Sie die einer Alarmregel zugeordneten Eigenschaften bearbeiten. Zum Aktivieren einer Alarmregel auf dieser Seite müssen Sie einen Alarmtyp, eine Alarmstufe und ein gültiges Alarmziel definieren.

Auf der Seite Alert Settings befindet sich ebenfalls die Schaltfläche Send Test Alert. Mithilfe dieser Funktion zum Testen von Alarmen können Sie überprüfen, ob alle in einer aktivieren Alarmregel angegebenen Alarmempfänger eine Alarmmeldung empfangen.

**ABBILDUNG 7-9** Seite Alert Settings


System Management Access
Alert Management
Network
Serial Port
Clock Settings
Syslog
SMTP Client
Policy
Alert Settings
This shows the table of configured alerts. To send a test alert to each of the configured alert destinations, click the Send Test Alerts button. IPMI Platform Event Traps (PETs), Email Alerts and SNMP Traps are supported. Select a radio button, then select Edit from the Actions drop down list to configure an alert. You can configure up to 15 alerts.
Send Test Alerts
Alerts
— Actions —
Alert ID
Level
Alert Type
Destination Summary
1 disable ipmipet 0.0.0.0
2 disable ipmipet 0.0.0.0
3 disable ipmipet 0.0.0.0
4 disable ipmipet 0.0.0.0
5 disable ipmipet 0.0.0.0
6 disable ipmipet 0.0.0.0
7 disable ipmipet 0.0.0.0
8 disable ipmipet 0.0.0.0
9 disable ipmipet 0.0.0.0
10 disable ipmipet 0.0.0.0
11 disable ipmipet 0.0.0.0
12 disable ipmipet 0.0.0.0
13 disable ipmipet 0.0.0.0
14 disable ipmipet 0.0.0.0
15 disable ipmipet 0.0.0.0

Zusätzliche Information zum Erstellen und Verwalten von Alarmregelkonfigurationen in ILOM mithilfe der Webbenutzeroberfläche finden Sie in den folgenden Abschnitten:

- „Voraussetzungen“ auf Seite 146.
- „Ändern von Alarmregelkonfigurationen mithilfe der Webbenutzeroberfläche“ auf Seite 146.
- „Deaktivieren von Alarmregelkonfigurationen mithilfe der Webbenutzeroberfläche“ auf Seite 147.
- „Erzeugen von Alarmtests mithilfe der Webbenutzeroberfläche“ auf Seite 148.

## Voraussetzungen

- Beim Definieren eines E-Mail-Benachrichtigungsalarms muss der ausgehende E-Mail-Server, der zum Senden der E-Mail-Benachrichtigung verwendet wird, in ILOM konfiguriert sein. Ist ein ausgehender E-Mail-Server nicht konfiguriert, kann ILOM keine E-Mail-Benachrichtigungsalarme erfolgreich erzeugen.
- Beim Definieren eines SNMP-Trap-Alarms mit der Version „SNMP v3“ muss der SNMP-Benutzername in ILOM als SNMP-Benutzer definiert sein. Ist der Benutzer nicht in ILOM als SNMP-Benutzer definiert, kann der SNMP-Alarmbenutzer die SNMP-Alarmmeldung nicht dekodieren. Weitere Informationen zum Definieren von SNMP-Benutzern in ILOM finden Sie in Kapitel 10.
- Zum Erstellen, Ändern oder Deaktivieren einer Alarmregel in ILOM müssen Sie sich bei ILOM mit einem Administratorkonto anmelden.

## ▼ Ändern von Alarmregelkonfigurationen mithilfe der Webbenutzeroberfläche

Mithilfe des folgenden Verfahrens können Sie eine Alarmregelkonfiguration in ILOM ändern:

1. **Öffnen Sie einen Webbrowser, und geben Sie die IP-Adresse des Server-SP oder CMM ein.**

   Die Anmeldeseite der ILOM-Webbenutzeroberfläche wird angezeigt.

2. **Geben Sie auf der Seite ILOM Login einen Administrator-Benutzernamen mit Passwort ein, und klicken Sie auf OK.**

   Die ILOM-Webbenutzeroberfläche wird angezeigt.

3. **Wählen Sie auf der Webbenutzeroberflächenseite Configuration --> Alert Management.**

**Hinweis –** Alternativ können Alarmregelkonfigurationen für einen Server-SP über die CMM-Webbenutzeroberfläche verwaltet werden. Zum Verwalten einer Alarmregelkonfiguration für einen Server-SP über das CMM wählen Sie zuerst im linken Rahmen der Seite den Server-SP (Blade) aus und klicken dann im rechten Rahmen der Seite auf Configuration -->Alert Management.

Die Seite Alert Settings wird angezeigt.

4. **Führen Sie auf der Seite Alert Settings Folgendes aus:**

   a. **Aktivieren Sie das Optionsfeld für die Alarmregel, die erstellt oder bearbeitet werden soll.**

   b. **Wählen Sie im Dropdown-Listenfeld Actions den Eintrag Edit.**

      Ein Dialogfeld mit den Eigenschaftenwerten, die der Alarmregel zugeordnet sind, wird angezeigt.

   c. **Geben Sie im Dialogfeld Properties Werte für einen Alarmtyp (Alert Type), eine Alarmstufe (Alert Level) und ein Alarmziel (Alert Destination) an.**

      Wenn es sich bei dem angegebenen Alarmtyp um eine SNMP-Trap handelt, können Sie optional einen Community Name- oder User Name-Wert definieren, um den Empfang der Alarmmeldung zu authentifizieren.

      Weitere Informationen zu den Eigenschaftenwerten, die für eine Alarmregel angegeben werden können, finden Sie unter „Eigenschaften zum Definieren von Alarmregeln“ auf Seite 142.

   d. **Klicken Sie auf Save, um die angegebenen Werte zu übernehmen und das Dialogfeld Properties zu schließen.**

## ▼ Deaktivieren von Alarmregelkonfigurationen mithilfe der Webbenutzeroberfläche

Mithilfe des folgenden Verfahrens können Sie eine Alarmregelkonfiguration in ILOM deaktivieren:

1. **Öffnen Sie einen Webbrowser, und geben Sie die IP-Adresse des Server-SP oder CMM ein.**

   Die Anmeldeseite der ILOM-Webbenutzeroberfläche wird angezeigt.

2. **Geben Sie auf der Seite ILOM Login einen Administrator-Benutzernamen mit Passwort ein, und klicken Sie auf OK.**

   Die ILOM-Webbenutzeroberfläche wird angezeigt.

3. **Wählen Sie auf der Webbenutzeroberflächenseite Configuration --> Alert Management.**

---

**Hinweis –** Alternativ können Alarmregelkonfigurationen für einen Server-SP über die CMM-Webbenutzeroberfläche verwaltet werden. Zum Verwalten einer Alarmregelkonfiguration für einen Server-SP über das CMM wählen Sie zuerst im linken Rahmen der Seite den Server-SP (Blade) aus und klicken dann im rechten Rahmen der Seite auf Configuration -->Alert Management.

---

Die Seite Alert Settings wird angezeigt.

4. **Aktivieren Sie auf der Seite Alert Settings das Optionsfeld für die Alarmregel, die geändert werden soll, und klicken Sie dann im Dropdown-Listenfeld Actions auf Edit.**

   Ein Dialogfeld mit Eigenschaften, die für die Alarmregel definiert werden können, wird angezeigt.

5. **Wählen Sie im Dialogfeld Properties im Dropdown-Listenfeld Alert Levels den Eintrag Disabled aus.**

## ▼ Erzeugen von Alarmtests mithilfe der Webbenutzeroberfläche

Jede *aktivierte* Alarmregelkonfiguration kann in ILOM durch Senden eines Testalarms getestet werden. Zum Erzeugen eines Testalarms für in Alarmregelkonfigurationen von ILOM angegebene Ziele verwenden Sie folgendes Verfahren:

1. **Öffnen Sie einen Webbrowser, und geben Sie die IP-Adresse des Server-SP oder CMM ein.**

   Die Anmeldeseite der ILOM-Webbenutzeroberfläche wird angezeigt.

2. **Geben Sie auf der Seite ILOM Login einen Administrator-Benutzernamen mit Passwort ein, und klicken Sie auf OK.**

   Die ILOM-Webbenutzeroberfläche wird angezeigt.

3. **Wählen Sie auf der Webbenutzeroberflächenseite Configuration --> Alert Management.**

**Hinweis –** Alternativ können Alarmregelkonfigurationen für einen Server-SP über die CMM-Webbenutzeroberfläche verwaltet werden. Zum Verwalten einer Alarmregelkonfiguration für einen Server-SP über das CMM wählen Sie zuerst im linken Rahmen der Seite den Server-SP (Blade) aus und klicken dann im rechten Rahmen der Seite auf Configuration -->Alert Management.

Die Seite Alert Settings wird angezeigt.

4. **Auf der Seite Alert Settings klicken Sie auf die Schaltfläche Send Test Alert.**

   ILOM erzeugt Testalarme für alle auf der Seite Alert Settings aktivierten Alarmregelkonfigurationen.

# Verwalten von Alarmregelkonfigurationen mithilfe der ILOM-CLI

Alle Alarmregelkonfigurationen können in ILOM über die Befehlszeilenschnittstelle (CLI) aktiviert, geändert und deaktiviert werden. Alle 15 in ILOM definierten Alarmregelkonfigurationen sind standardmäßig deaktiviert. Zum Aktivieren von Alarmregelkonfigurationen in ILOM müssen für folgende Eigenschaften Werte festgelegt werden: Alert Type, Alert Level und Alert Destination.

Testalarme können ebenfalls für alle in ILOM *aktivierten* Alarmregelkonfigurationen über die CLI erzeugt werden. Mithilfe dieser Funktion zum Testen von Alarmen können Sie überprüfen, ob alle in einer *aktivieren* Alarmregelkonfiguration angegebenen Alarmempfänger die Alarmmeldung empfangen.

Weitere Information zum Verwalten und Erstellen von Alarmregelkonfigurationen in ILOM mithilfe der CLI finden Sie in den folgenden Abschnitten:


- „CLI-Befehle zum Verwalten von Alarmregelkonfigurationen“ auf Seite 150
- „Voraussetzungen“ auf Seite 152
- „Ändern von Alarmregelkonfigurationen mithilfe der CLI“ auf Seite 152
- „Deaktivieren von Alarmregelkonfigurationen mithilfe der CLI“ auf Seite 153
- „Erzeugen von Alarmtests mithilfe der CLI“ auf Seite 154

# CLI-Befehle zum Verwalten von Alarmregelkonfigurationen

In TABELLE 7-2 werden CLI-Befehle aufgeführt, die üblicherweise zum Verwalten von Alarmregelkonfigurationen mithilfe der ILOM-CLI verwendet werden müssen.

**TABELLE 7-2** CLI-Befehle zum Verwalten von Alarmregelkonfigurationen

| CLI-Befehl | Beschreibung |
|---|---|
| `show` | Mit dem Befehl `show` können Sie jede Ebene der Struktur der Befehle für die Alarmverwaltung anzeigen, indem entweder der vollständige (absolute) oder der relative Pfad angegeben wird.<br>**Beispiele:**<br>• Zum Anzeigen einer Alarmregel mit ihren Eigenschaften mithilfe eines vollständigen (absoluten) Pfads würden Sie Folgendes an der Befehlseingabeaufforderung eingeben:<br>**`show /SP/alertmgmt/rules/1`**<br>`/SP/alertmgmt/rules/1`<br>`Properties:`<br>`community_or_username = public`<br>`destination = 129.148.185.52`<br>`level = minor`<br>`snmp_version = 1`<br>`type = snmptrap`<br>`Commands:`<br>`cd`<br>`set`<br>`show`<br>• Zum Anzeigen einer einzelnen Eigenschaft mithilfe des vollständigen (absoluten) Pfads würden Sie Folgendes an der Befehlseingabeaufforderung eingeben:<br>**`show /SP/alertmgmt/rules/1 type`**<br>`Properties:`<br>`type = snmptrap`<br>`Commands:`<br>`set`<br>`show` |

**TABELLE 7-2** CLI-Befehle zum Verwalten von Alarmregelkonfigurationen *(Fortsetzung)*

| CLI-Befehl | Beschreibung |
|---|---|
| | • Zum Angeben eines relativen Pfads würden Sie folgenden Befehl an der Befehlseingabeaufforderung eingeben, wenn die aktuelle Position in der Struktur `/SP/alertmgmt/rules` ist:<br>**`show 1/`**<br>`/SP/alertmgmt/rules/1`<br>`Targets:`<br>`Properties:`<br>`community_or_username = public`<br>`destination = 129.148.185.52`<br>`level = minor`<br>`snmp_version = 1`<br>`type = snmptrap`<br>`Commands:`<br>`cd`<br>`set`<br>`show` |
| `cd` | Mit dem Befehl `cd` können Sie das Arbeitsverzeichnis festlegen. Zum Festlegen der Alarmverwaltung als Arbeitsverzeichnis auf einem Server-SP würden Sie folgenden Befehl an der Befehlseingabeaufforderung eingeben:<br>**`cd /SP/alertmgmt`** |
| `set` | Mit dem Befehl `set` können Sie Werte für Eigenschaften an einer beliebigen Position in der Struktur festlegen. In Abhängigkeit von der Position in der Struktur können Sie entweder einen vollständigen (abosluten) oder einen relativen Pfad für die Eigenschaft angeben. Beispiel:<br>• Bei einem vollständigen (absoluten) Pfad würden Sie folgenden Befehlspfad an der Befehlseingabeaufforderung eingeben:<br>**`set /SP/alertmgmt/rules/1 type=ipmipet`**<br>• Bei einem relativen Pfad (Position in der Struktur ist `/SP/alertmgmt`) würden Sie folgenden Befehlspfad an der Befehlseingabeaufforderung eingeben:<br>**`set rules/1 type=ipmipet`**<br>• Bei einem relativen Pfad (Position in der Struktur ist `/SP/alertmgmt/rules/1`) würden Sie folgenden Befehlspfad an der Befehlseingabeaufforderung eingeben:<br>**`set type=ipmipet`** |

## Voraussetzungen

- Beim Definieren eines E-Mail-Benachrichtigungsalarms muss der ausgehende E-Mail-Server, der zum Senden der E-Mail-Benachrichtigung verwendet wird, in ILOM konfiguriert sein. Ist ein ausgehender E-Mail-Server nicht konfiguriert, kann ILOM keine E-Mail-Benachrichtigungsalarme erfolgreich erzeugen.
- Beim Definieren eines SNMP-Trap-Alarms mit der Version „SNMP v3“ muss der SNMP-Benutzername in ILOM als SNMP-Benutzer definiert sein. Ist der Benutzer nicht in ILOM als SNMP-Benutzer definiert, kann der SNMP-Alarmbenutzer die SNMP-Alarmmeldung nicht dekodieren. Weitere Informationen zum Definieren von SNMP-Benutzern in ILOM finden Sie in Kapitel 10.
- Zum Erstellen, Ändern oder Deaktivieren einer Alarmregel in ILOM müssen Sie sich bei ILOM mit einem Administratorkonto anmelden.

## ▼ Ändern von Alarmregelkonfigurationen mithilfe der CLI

1. **Stellen Sie eine lokale serielle Konsolenverbindung oder eine SSH-Verbindung mit dem Server-SP oder CMM her.**
   - **Lokale serielle Konsolenverbindung**

     **Schließen Sie eine serielle Konsole am seriellen Anschluss des Servers oder des CMM an**.

     Weitere Informationen finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

   oder

   - **Entfernte SSH-Verbindung (Secure Shell)**

     **Stellen Sie eine SSH-Verbindung mit dem Server-SP oder CMM her**.

     Stellen Sie von dem entfernten Client aus eine sichere Verbindung als root-Benutzer mit dem Server-SP oder dem aktiven CMM her.

     Sie können beispielsweise eine sichere Verbindung von einem entfernten SSH-Client aus mit dem Server-SP herstellen, indem Sie Folgendes eingeben:

     **`ssh -l root`** *server_ip_adresse*

     `Passwort:` **`changeme`**

     Die Standard-Befehlseingabeaufforderung wird angezeigt (->).

2. **Geben Sie einen der folgenden Befehlspfade ein, um das Arbeitsverzeichnis festzulegen:**
   - Bei einem Rack-System-Server: **`cd /SP/alertmgmt`**
   - Bei einem Blade-Servermodul: **`cd /SP/alertmgmt`**
   - Bei einem Gehäuse-CMM: **`cd /CMM/alertmgmt`**

3. **Geben Sie den Befehl** `show` **ein, um die Eigenschaften anzuzeigen, die einer Alarmregel zugeordnet sind.**

   Um beispielsweise die der ersten Alarmregel zugeordneten Eigenschaften anzuzeigen, würden Sie eine der folgenden Eingaben vornehmen:

   - Bei einem Rack-System-Server: **`show /SP/alertmgmt/rules/1`**
   - Bei einem Blade-Servermodul: **`show /CH/BL`*n*`/SP/alertmgmt/rules/1`**
   - Bei einem Gehäuse-CMM: **`show /CMM/alertmgmt/CMM/rules/1`**

4. **Geben Sie den Befehl** `set` **ein, um den einer Alarmregel zugeordneten Eigenschaften Werte zuzuweisen.**

   Um beispielsweise IPMI PET als Alarmtyp (Alert Type) für Regel 1 festzulegen, würden Sie folgende Befehlspfade eingeben:

   **`set type=ipmipet`**

---

**Hinweis –** Zum Aktivieren einer Alarmregelkonfiguration müssen Sie einen Wert für den Alarmtyp, die Alarmstufe und das Alarmziel angeben. Beim Definieren eines SNMP-Alarmtyps können Sie optional einen Wert zum Authentifizieren des Empfangs von SNMP-Trap-Alarmen definieren.

---

Weitere Informationen zu den einzelnen Eigenschaftenwerten, die für eine Alarmregel definiert werden können, finden Sie in TABELLE 7-1 „Eigenschaften zum Definieren von Alarmregeln“ auf Seite 142.

## ▼ Deaktivieren von Alarmregelkonfigurationen mithilfe der CLI

Mithilfe des folgenden Verfahrens können Sie Alarmregelkonfigurationen in ILOM über die CLI deaktivieren:

1. **Stellen Sie eine lokale serielle Konsolenverbindung oder eine SSH-Verbindung mit dem Server-SP oder CMM her.**

   - **Lokale serielle Konsolenverbindung**

     **Schließen Sie eine serielle Konsole am seriellen Anschluss des Servers oder des CMM an**.

     Weitere Informationen finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

   oder

   - **Entfernte SSH-Verbindung (Secure Shell)**

     **Stellen Sie eine SSH-Verbindung mit dem Server-SP oder CMM her**.

Stellen Sie von dem entfernten Client aus eine sichere Verbindung als root-Benutzer mit dem Server-SP oder dem aktiven CMM her.

Sie können beispielsweise eine sichere Verbindung von einem entfernten SSH-Client aus mit dem Server-SP herstellen, indem Sie Folgendes eingeben:

**`ssh -l root`** *server_ip_adresse*

`Passwort:` **`changeme`**

Die Standard-Befehlseingabeaufforderung wird angezeigt (->).

2. **Legen Sie mithilfe des Befehls `cd` das Arbeitsverzeichnis auf die Alarmverwaltungsregel fest, die deaktiviert werden soll.**

   Beispiel:

   - Geben Sie bei einem Rack-System-Server-SP Folgendes ein: **`cd /SP/alertngnt/rules/`***n*
   - Geben Sie bei einem Blade-Server-SP Folgendes ein: **`cd /CH/BL`***n***`/SP/alertmgmt/rules/`***n*
   - Geben Sie bei einem Gehäuse-CMM Folgendes ein: **`cd /CMM/alertmgmt/CMM/rules/`***n*

     wobei *n* die Nummer einer bestimmten Alarmregel aus dem Bereich 1–15 ist.

3. **Geben Sie zum Deaktivieren der Alarmregel folgenden Befehl ein:**

   **`set level=disable`**

# ▼ Erzeugen von Alarmtests mithilfe der CLI

Jede *aktivierte* Alarmregelkonfiguration kann in ILOM durch Senden eines Testalarms getestet werden.
Zum Erzeugen eines Testalarms für in Alarmregelkonfigurationen von ILOM angegebene Ziele verwenden Sie folgendes Verfahren:

1. **Stellen Sie eine lokale serielle Konsolenverbindung oder eine SSH-Verbindung mit dem Server-SP oder CMM her.**

   - **Lokale serielle Konsolenverbindung**

     **Schließen Sie eine serielle Konsole am seriellen Anschluss des Servers oder des CMM an**.

     Weitere Informationen finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

   oder

   - **Entfernte SSH-Verbindung (Secure Shell)**

     **Stellen Sie eine SSH-Verbindung mit dem Server-SP oder CMM her**.

Stellen Sie von dem entfernten Client aus eine sichere Verbindung als root-Benutzer mit dem Server-SP oder dem aktiven CMM her.

Sie können beispielsweise eine sichere Verbindung von einem entfernten SSH-Client aus mit dem Server-SP herstellen, indem Sie Folgendes eingeben:

**`ssh -l root`** *server_ip_adresse*

`Passwort:` **`changeme`**

Die Standard-Befehlseingabeaufforderung wird angezeigt (->).

2. **Legen Sie mithilfe des Befehls `cd` das Arbeitsverzeichnis auf die Alarmverwaltungsregeln fest.**

   Beispiel:

   - Geben Sie bei einem Rack-System-Server-SP Folgendes ein: **`cd /SP/alertmgmt/rules`**
   - Geben Sie bei einem Blade-Server-SP Folgendes ein: **`cd /CH/BL`***n*`/SP/alertmgmt/rules`**
   - Geben Sie bei einem Gehäuse-CMM Folgendes ein: **`cd /CMM/alertmgmt/CMM/rules`**

3. **Geben Sie folgenden Befehl ein, um einen Testalarm zu erzeugen:**

   **`set testalert=true`**

# Konfigurieren eines SMTP-Clients für E-Mail-Benachrichtigungsalarme

Zum Erzeugen konfigurierter E-Mail-Benachrichtigungsalarme müssen Sie den ILOM-Client so konfigurieren, dass er als SMTP-Client zum Senden der E-Mail-Alarmmeldung fungieren kann. Um den ILOM-Client als SMTP-Client zu aktivieren, müssen Sie die IP-Adresse und Anschlussnummer eines ausgehenden SMTP-E-Mail-Servers angeben, von dem die E-Mail-Benachrichtigungen verarbeitet werden sollen.

Weitere Information zum Konfigurieren eines SMTP-Clients für E-Mail-Benachrichtigungsalarme in ILOM finden Sie in den folgenden Abschnitten:


- „Aktivieren eines SMTP-Clients mithilfe der Webbenutzeroberfläche“ auf Seite 156
- „Aktivieren eines SMTP-Clients mithilfe der CLI“ auf Seite 156


**Voraussetzung:**

- Vor dem Aktivieren des ILOM-Clients als SMTP-Client müssen Sie die IP-Adresse und Anschlussnummer des ausgehenden SMTP-E-Mail-Servers herausfinden.

## ▼ Aktivieren eines SMTP-Clients mithilfe der Webbenutzeroberfläche

Führen Sie diese Schritte durch, um in ILOM mithilfe der Webbenutzeroberfläche einen SMTP-Client zu konfigurieren:

1. **Öffnen Sie einen Webbrowser, und geben Sie die IP-Adresse des Server-SP oder CMM ein.**

   Die Anmeldeseite der ILOM-Webbenutzeroberfläche wird angezeigt.

2. **Geben Sie auf der Seite ILOM Login einen Administrator-Benutzernamen mit Passwort ein, und klicken Sie auf OK.**

   Die ILOM-Webbenutzeroberfläche wird angezeigt.

3. **Wählen Sie auf der Webbenutzeroberflächenseite Configuration --> SMTP Client.**
4. **Geben Sie auf der Seite SMTP Client die folgenden Einstellungen an, um das Senden von E-Mail-Benachrichtigungsalarmen zu aktivieren.**

| SMTP-Einstellung | Beschreibung |
|---|---|
| SMTP State | Aktivieren Sie das Kontrollkästchen, um diesen Zustand zu aktivieren. |
| SMTP Server IP | Geben Sie die IP-Adresse des ausgehenden SMTP-E-Mail-Servers ein, von dem die E-Mail-Benachrichtigungen verarbeitet werden sollen. |
| SMTP Port | Geben Sie die Anschlussnummer des ausgehenden SMTP-E-Mail-Servers ein. |

5. **Klicken Sie auf Save, um die SMTP-Einstellungen zu übernehmen.**

## ▼ Aktivieren eines SMTP-Clients mithilfe der CLI

Führen Sie diese Schritte durch, um in ILOM mithilfe der CLI einen SMTP-Client zu konfigurieren:

1. **Stellen Sie eine lokale serielle Konsolenverbindung oder eine SSH-Verbindung mit dem Server-SP oder CMM her.**
   - **Lokale serielle Konsolenverbindung**

     **Schließen Sie eine serielle Konsole am seriellen Anschluss des Servers oder des CMM an**.

     Weitere Informationen finden Sie in der Benutzerdokumentation, die der jeweiligen Serverplattform beiliegt.

   oder

- **Entfernte SSH-Verbindung (Secure Shell)**

  **Stellen Sie eine SSH-Verbindung mit dem Server-SP oder CMM her.**

  Stellen Sie von dem entfernten Client aus eine sichere Verbindung als root-Benutzer mit dem Server-SP oder dem aktiven CMM her.

  Sie können beispielsweise eine sichere Verbindung von einem entfernten SSH-Client aus mit dem Server-SP herstellen, indem Sie Folgendes eingeben:

  **`ssh -l root`** *server_ip_adresse*

  `Passwort:` **`changeme`**

  Die Standard-Befehlseingabeaufforderung wird angezeigt (->).

2. **Legen Sie mithilfe des Befehls `cd` das Arbeitsverzeichnis auf `clients/smtp` fest.**

   Beispiel:

   - Geben Sie bei einem Rack-System-Server-SP Folgendes ein: **`cd /SP/clients/smtp`**
   - Geben Sie bei einem Blade-Server-SP Folgendes ein: **`cd /CH/BL`***n*`/SP/clients/smtp`**
   - Geben Sie bei einem Gehäuse-CMM Folgendes ein: **`cd /CMM/clients/smtp`**

3. **Geben Sie den Befehl `show` ein, um die SMTP-Eigenschaften anzuzeigen.**

   Beim ersten Zugriff auf die SMTP-Eigenschaften auf einem SP würde ungefähr Folgendes angezeigt:

```
show
/SP/clients/smtp
Targets
  Properties
  address = 0. 0. 0. 0
  port = 25
  state = enabled
Commands:
  cd
  set
  show
```

4. **Geben Sie mithilfe des Befehls `set` eine IP-Adresse für den SMTP-Client an, oder ändern Sie mit diesem Befehl den Wert für die Anschluss- oder Zustandeigenschaft.**

   Beispiel:

   `set address=222.333.44.5`

5. **Drücken Sie die Eingabetaste, um die Änderung zu übernehmen.**

   Würde beispielsweise `set address=222.333.44.5` eingegeben, würde folgendes Ergebnis angezeigt:

   ```
   Set 'address=222.333.44.5'
   ```

KAPITEL 8

# Konfigurieren von ILOM-Kommunikationseinstellungen

Zu den erweiterten ILOM-Kommunikationseinstellungen zählen unter anderem Netzwerk-, serielle Anschluss- und Webkonfiguration.

Dieses Kapitel enthält folgende Abschnitte:


- „Verwalten von ILOM-Netzwerkeinstellungen mithilfe der CLI“ auf Seite 160
  - „Anzeigen von Netzwerkeinstellungen mithilfe der CLI“ auf Seite 161
  - „Konfigurieren von Netzwerkeinstellungen mithilfe der CLI“ auf Seite 161
  - „Anzeigen von seriellen Anschlusseinstellungen mithilfe der CLI“ auf Seite 163
  - „Konfigurieren von seriellen Anschlusseinstellungen mithilfe der CLI“ auf Seite 163
  - „Aktivieren von HTTP- oder HTTPS-Webzugriff mithilfe der CLI“ auf Seite 164
- „Konfigurieren von SSH-Einstellungen (Secure Shell)“ auf Seite 166
  - „Herstellen einer sicheren entfernten Verbindung zum Ausführen von CLI-Befehlen“ auf Seite 166
  - „Anzeigen des aktuellen Schlüssels mithilfe der CLI“ auf Seite 166
  - „Aktivieren und Deaktivieren der SSH mithilfe der CLI“ auf Seite 168
  - „Aktivieren und Deaktivieren der SSH mithilfe der Webbenutzeroberfläche“ auf Seite 168
  - „Erzeugen eines neuen Schlüssels mithilfe der CLI“ auf Seite 169
  - „Erzeugen eines neuen Schlüssels mithilfe der Webbenutzeroberfläche“ auf Seite 169
  - „Neustart des SSH-Servers mithilfe der CLI“ auf Seite 169
  - „Neustart des SSH-Servers mithilfe der Webbenutzeroberfläche“ auf Seite 170
- „Verwalten von ILOM-Netzwerkeinstellungen mithilfe der Webbenutzeroberfläche“ auf Seite 170
  - „Anzeigen von Netzwerkeinstellungen mithilfe der Webbenutzeroberfläche“ auf Seite 170

- „Konfigurieren von Netzwerkeinstellungen mithilfe der Webbenutzeroberfläche“ auf Seite 171
- „Anzeigen von seriellen Anschlusseinstellungen mithilfe der Webbenutzeroberfläche“ auf Seite 172
- „Konfigurieren von seriellen Anschlusseinstellungen mithilfe der Webbenutzeroberfläche“ auf Seite 173
- „Aktivieren von HTTP- oder HTTPS-Webzugriff mithilfe der Webbenutzeroberfläche“ auf Seite 174


**Hinweis –** In diesem Kapitel verwendete Syntaxbeispiele verwenden das Ziel beginnend mit `/SP/`. Dies könnte in Abhängigkeit von der verwendeten Serverplattform gegen das Ziel beginnend mit `/CMM/` ausgetauscht werden. Unterziele sind auf allen Serverplattformen gleich.

# Verwalten von ILOM-Netzwerkeinstellungen mithilfe der CLI

In diesem Abschnitt wird beschrieben, wie die Netzwerkeinstellungen für ILOM mithilfe der ILOM-CLI konfiguriert werden.

## Informationen zu Netzwerkeinstellungen

Netzwerkeinstellungen verfügen über zwei Sätze von Eigenschaften: anstehend (pending) und aktiv. Die aktiven Einstellungen werden aktuell von ILOM verwendet Sie sind schreibgeschützt. Wenn Sie Einstellungen ändern möchten, geben Sie die aktualisierten Einstellungen als anstehende Einstellungen ein (`pendingipaddress` oder `pendingipgateway`) und legen dann die Eigenschaft `commitpending` auf `true` fest. Auf diese Weise verhindern Sie versehentliche Unterbrechungen bei Anschluss und Netzwerkeinstellungen.

**Hinweis –** Stellen Sie sicher, dass ILOM immer dieselbe IP-Adresse zugewiesen ist, indem Sie ILOM nach dem ersten Einrichten eine statische IP-Adresse zuweisen, oder indem Sie den DHCP-Server so konfigurieren, dass ILOM immer dieselbe IP-Adresse zugewiesen wird. So kann ILOM leicht im Netzwerk gefunden werden.

## ▼ Anzeigen von Netzwerkeinstellungen mithilfe der CLI

1. **Melden Sie sich bei der ILOM-CLI als Administrator oder Operator an.**
2. **Geben Sie an der Befehlseingabeaufforderung Folgendes ein:**

```
-> show /SP/network
```

## ▼ Konfigurieren von Netzwerkeinstellungen mithilfe der CLI

Mit dem Befehl `set` können Sie Eigenschaften und Werte für Netzwerkeinstellungen ändern.

1. **Melden Sie sich bei der ILOM-CLI als Administrator an.**
2. **Geben Sie an der Befehlseingabeaufforderung Folgendes ein:**

```
-> set /SP/network
```

### Ziele, Eigenschaften und Werte

Folgende Ziele, Eigenschaften und Werte sind für ILOM-Netzwerkeinstellungen gültig.

**TABELLE 8-1** ILOM-Netzwerkziele, -eigenschaften und -werte

| Ziel | Eigenschaft | Wert | Standard |
|---|---|---|---|
| **/SP/network** | ipaddress<br>ipdiscovery<br>ipgateway<br>ipnetmask | Diese schreibgeschützten Werte werden vom System aktualisiert. | |
| | macaddress | Die MAC-Adresse von ILOM. | |
| | commitpending | true\|(none) | (none) |
| | pendingipaddress | <*ipadresse*\|none> | none |
| | pendingipdiscovery | dhcp\|static | dhcp |
| | pendingipgateway | <*ipadresse*\|none> | none |
| | pendingipnetmask | <*ipdotteddecimal*> | 255.255.255.255 |

*Beispiel*

Geben Sie zum Ändern der IP-Adresse für ILOM Folgendes ein:

```
-> set /SP/network pendingipaddress=nnn.nn.nn.nn commitpending=true
```

---

**Hinweis –** Durch das Ändern der IP-Adresse wird die aktive Sitzung unterbrochen, wenn Sie mit ILOM über ein Netzwerk verbunden sind.

---

Geben Sie zum Ändern der Netzwerkeinstellungen von DHCP- in statische Zuweisung Folgendes ein:

```
-> set /SP/network pendingipdiscovery=static pendingipaddress=
nnn.nn.nn.nn pendingipgateway=nnn.nn.nn.nn pendingipnetmask=nnn.nn.nn.nn
commitpending=true
```

---

**Hinweis –** Die Einstellungen werden übernommen und somit aktiv, sobald `commitpending` auf `true` festgelegt wird.

---

# Serielle Anschlusseinstellungen

Der serielle Anschluss bietet Zugriff auf die ILOM-Webbenutzeroberfläche, die CLI (Command-Line Interface) und den Systemkonsolenstream mithilfe der Umleitung des seriellen Anschlusses.

- Der interne serielle Anschluss ist die Verbindung zwischen dem Hostserver und ILOM, die es einem ILOM-Benutzer ermöglicht, auf die serielle Hostkonsole zuzugreifen. Die Geschwindigkeit des internen seriellen ILOM-Anschlusses muss mit der Geschwindigkeit des Anschlusses der seriellen Konsole am Hostserver, häufig als serieller Anschluss 0, COM1 oder /dev/ttyS0 bezeichnet, übereinstimmen.

---

**Hinweis –** Normalerweise stimmen die Einstellungen der seriellen Hostkonsole mit den Standardeinstellungen von ILOM überein (9600 Baud, 8N1 [acht Daten-Bits, keine Parität, ein Stopp-Bit], keine Flusssteuerung).

---

- Der externe serielle Anschluss ist der serielle RJ-45-Anschluss an ILOM. Üblicherweise müssen die internen und externen seriellen Anschlussverbindungen mit derselben Geschwindigkeit arbeiten, um Flusssteuerungsprobleme zu vermeiden, wenn über den externen seriellen Anschluss von ILOM eine Verbindung mit der Hostkonsole hergestellt wird.

## ▼ Anzeigen von seriellen Anschlusseinstellungen mithilfe der CLI

1. **Melden Sie sich bei der ILOM-CLI als Administrator oder Operator an.**
2. **Geben Sie an der Befehlseingabeaufforderung Folgendes ein:**
   - Befehl zum Anzeigen von Einstellungen für den externen seriellen Anschluss:

     -> **show /SP/serial/external**
   - Befehl zum Anzeigen von Einstellungen für den seriellen Hostanschluss:

     -> **show /SP/serial/host**

## ▼ Konfigurieren von seriellen Anschlusseinstellungen mithilfe der CLI

Mit dem Befehl `set` können Sie Eigenschaften und Werte für serielle Anschlusseinstellungen ändern. Anschlusseinstellungen verfügen über zwei Sätze von Eigenschaften: anstehend (pending) und aktiv. Die aktiven Einstellungen sind die Einstellungen, die aktuell von ILOM verwendet werden. Sie sind schreibgeschützt. Wenn Sie Einstellungen ändern möchten, geben Sie die aktualisierten Einstellungen als anstehende Einstellungen ein und legen dann die Eigenschaft `commitpending` auf `true` fest. Auf diese Weise verhindern Sie versehentliche Unterbrechungen bei Anschluss und Netzwerkeinstellungen.

1. **Melden Sie sich bei der ILOM-CLI als Administrator oder Operator an.**
2. **Geben Sie an der Befehlseingabeaufforderung Folgendes ein:**

-> **set target [propertyname=value]**

## Ziele, Eigenschaften und Werte

Folgende Ziele, Eigenschaften und Werte sind für serielle ILOM-Anschlüsse gültig.

**TABELLE 8-2** Gültige Ziele, Eigenschaften und Werte für serielle ILOM-Anschlüsse

| Ziel | Eigenschaft | Wert | Standard |
|---|---|---|---|
| **/SP/serial/external** | commitpending | true\|(none) | (none) |
| | flowcontrol | none | none |
| | pendingspeed | <*Dezimalzahl*> | 9600 |
| | speed | 9600 | 9600 |
| **/SP/serial/host** | commitpending | true\|(none) | (none) |
| | pendingspeed | <*Dezimalzahl*> | (none) |
| | speed | 9600 | 9600 |

### *Beispiel*

Geben Sie zum Ändern der Geschwindigkeit (Baudrate) für den seriellen Hostanschluss von 9600 in 57600 Folgendes ein:

```
-> set /SP/serial/host pendingspeed=57600 commitpending=true
```

---

**Hinweis –** Die Geschwindigkeit des seriellen Hostanschlusses muss mit der Geschwindigkeitseinstellung für den seriellen Anschluss 0, COM1 oder /dev/ttys0 des Hostbetriebssystems für ILOM übereinstimmen, damit ILOM ordnungsgemäß mit dem Host kommunizieren kann.

---

# ▼ Aktivieren von HTTP- oder HTTPS-Webzugriff mithilfe der CLI

ILOM unterstützt sowohl HTTP- als auch HTTPS-Verbindungen. ILOM ermöglicht das automatische Umleiten von HTTP-Zugriff auf HTTPS. ILOM ermöglicht außerdem das Festlegen der HTTP- und HTTPS-Anschlüse.

1. **Melden Sie sich bei der ILOM-CLI als Administrator an.**
2. **Geben Sie an der Befehlseingabeaufforderung Folgendes ein:**

   ```
   -> set /SP/services/http
   ```

   Die Eigenschaften befinden sich in /SP/services/http und /SP/services/https.

## Ziele, Eigenschaften und Werte

In TABELLE 8-3 finden Sie die gültigen Ziele, Eigenschaften und Werte für HTTP und HTTPS.

**TABELLE 8-3** Gültige Ziele, Eigenschaften und Werte für HTTP und HTTPS

| Ziel | Eigenschaft | Wert | Standard |
|---|---|---|---|
| /SP/services/http | secureredirect | enabled\| disabled | enabled |
| | servicestate | enabled\| disabled | disabled |
| | port | <*anschlussnum*> | 80 |
| /SP/services/https | servicestate | enabled\| disabled | enabled |
| | port | <*anschlussnum*> | 443 |

In TABELLE 8-4 werden die möglichen Einstellungen für HTTP, HTTPS und die automatische Umleitung aufgeführt.

**TABELLE 8-4** Mögliche Einstellungen für HTTP, HTTPS und automatische Umleitung

| Gewünschter Zustand | Ziel | Eigenschaft | Wert |
|---|---|---|---|
| Nur HTTP aktiviert | /SP/services/http | secureredirect | disabled |
| | /SP/services/http | servicestate | enabled |
| | /SP/services/https | servicestate | disabled |
| HTTP und HTTPS aktiviert | /SP/services/http | secureredirect | disabled |
| | /SP/services/http | servicestate | enabled |
| | /SP/services/https | servicestate | enabled |
| Nur HTTPS aktiviert | /SP/services/http | secureredirect | disabled |
| | /SP/services/http | servicestate | disabled |
| | /SP/services/https | servicestate | enabled |
| Automatische Umleitung von HTTP auf HTTPS | /SP/services/http | secureredirect | enabled |
| | /SP/services/http | servicestate | disabled |
| | /SP/services/https | servicestate | enabled |

# Konfigurieren von SSH-Einstellungen (Secure Shell)

Secure Shell (SSH) ist das Standardprotokoll für den Zugriff auf eine sichere entfernte Verbindung mit der ILOM-CLI. Durch das Verwenden der SSH ist sichergestellt, dass alle Verwaltungsinteraktionen mit ILOM verschlüsselt werden und sicher sind. Beide Enden der Serververbindung werden mithilfe digitaler Schlüssel authentifiziert, und Passwörter sind durch Verschlüsselung geschützt. Die ILOM-Verbindung ist durch Verschlüsselung mit RSA- und DSA-Schlüsseln geschützt.

## ▼ Herstellen einer sicheren entfernten Verbindung zum Ausführen von CLI-Befehlen

- **Sie müssen eine sichere Verbindung von einem entfernten SSH-Client aus mit dem Server-SP herstellen. Geben Sie zum Herstellen einer sicheren Verbindung Folgendes ein:**

  **`ssh -l`** *Benutzername server_ip_adresse*

  `Password:` **`********`**

  Die Standardeingabeaufforderung wird angezeigt (->), und das System ist jetzt zum Ausführen der CLI-Befehle bereit, um Netzwerkeinstellungen vorzunehmen.

## ▼ Anzeigen des aktuellen Schlüssels mithilfe der CLI

Die Notwendigkeit, Schlüssel anzuzeigen, erfordert eine erweiterte Konfiguration. In der Regel besteht keine Veranlassung zum Anzeigen von Schlüsseln. Sie können entweder den gesamten öffentlichen Schlüssel oder den abgekürzten Fingerabdruck (fingerprint) des Schlüssels anzeigen.

---

**Hinweis –** Alle unter `/SP/services/ssh/keys/`*rsa*|*dsa* aufgeführten Eigenschaften sind schreibgeschützt.

---

- **Geben Sie zum Anzeigen des RSA-Schlüssels Folgendes ein:**

```
-> show /SP/services/ssh/keys/rsa
    Beispiel:
/SP/services/ssh/keys/rsa
    Targets:
       Properties:
          fingerprint =
ca:c0:05:ff:b7:75:15:a0:30:df:1b:a1:76:bd:fe:e5
          length = 1024
           publickey
AAAAB3NzaC1yc2EAAAABIwAAAIEAthvlqgXbPIxN4OEvkukKupdFPr8GDaOsKGg
BESVlnny4nX8yd8JC/hrw3qDHmXIZ8JAFwoLQgjtZCbEsgpn9nNIMb6nSfu6Y1t
TtUZXSGFBZ48ROmU0SqqfR3i3bgDUR0siphlpgV6Yu0Zd1h3549wQ+RWk3vxqHQ
Ffzhv9c=
      Commands:
          cd
          show
```

- **Geben Sie zum Anzeigen des DSA-Schlüssels Folgendes ein:**

```
-> show /SP/services/ssh/keys/dsa
Beispiel:
 /SP/services/ssh/keys/dsa
     Targets:

     Properties:
        fingerprint =
6a:90:c7:37:89:e6:73:23:45:ff:d6:8e:e7:57:2a:60
        length = 1024
        publickey =
AAAAB3NzaC1kc3MAAACBAInrYecNH86imBbUqE+3FoUfm/fei2ZZtQzqrMx5zBm
bHFIaFdRQKeoQ7gqjc9jQbO7ajLxwk2vZzkg3ntnmqHz/hwHvdho2KaolBtAFGc
fLIdzGVxi4I3phVb6anmTlbqI2AILAa7JvQ8dEGbyATYR9A/pf5VTac/TQ70O/J
AAAAFQCIUavkex7wtEhC0CH3s25ON0I3CwAAAIBNfHUop6ZN7i46ZuQOKhD7Mkj
gdHy+8MTBkupVfXqfRE9Zw9yrBZCNsoD8XEeIeyP+puO5k5dJvkzqSqrTVoAXyY
qewyZMFE7stutugw/XEmyjq+XqBWaiOAQskdiMVnHa3MSg8PKJyWP8eIMxD3rIu
PTzkV632uBxzwSwfAQAAAIAtA8/3odDJUprnxLgHTowc8ksGBj/wJDgPfpGGJHB
B1FDBMhSsRbwh6Z+s/gAf1f+S67HJBTUPsVSMz+czmamc1oZeOazT4+zeNG6uCl
u/5/JmJSdkguc1FcoxtBFqfO/fKjyR0ecWaU7L4kjvWoSsydHJ0pMHasEecEBEr
lg==

     Commands:
         cd
         show
```

## ▼ Aktivieren und Deaktivieren der SSH mithilfe der CLI

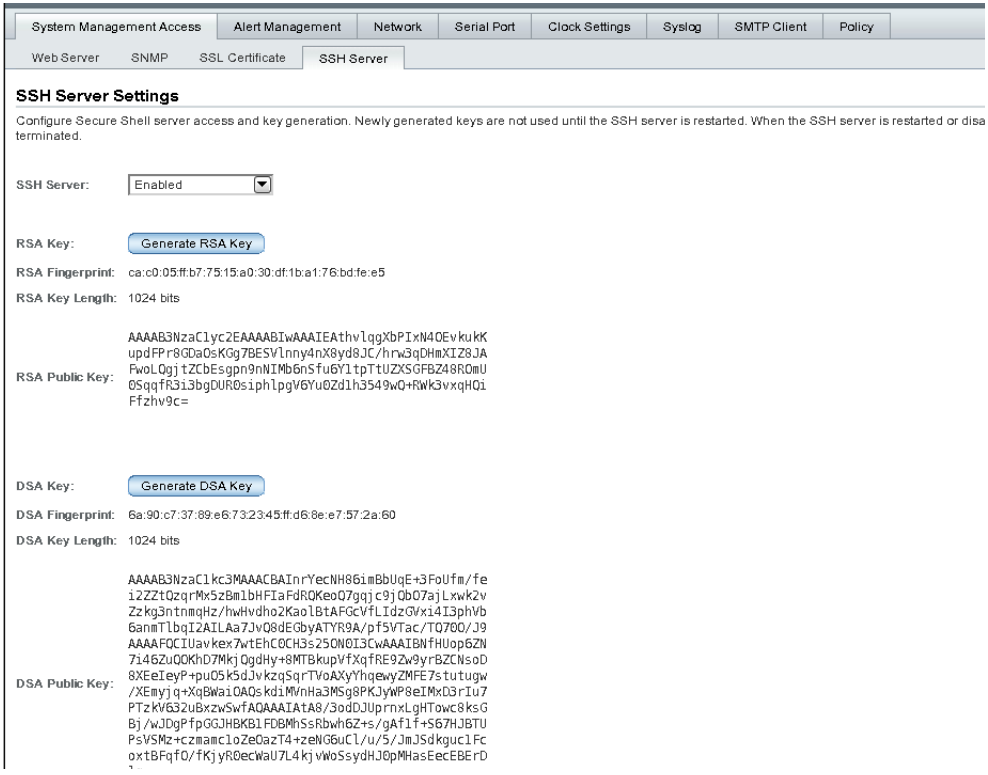
- **Wenn kein Zugriff über das Netzwerk bereitgestellt oder die SSH nicht verwendet werden soll, geben Sie Folgendes ein:**

```
-> set /SP/services/ssh state=enabled | disabled
```

## ▼ Aktivieren und Deaktivieren der SSH mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich bei ILOM als Administrator an.**
2. **Wählen Sie Configuration --> System Management Access --> SSH Server.**
3. **Wählen Sie im Dropdown-Listenfeld SSH Server den Eintrag Enabled oder Disabled.**

**ABBILDUNG 8-1** Seite SSH Server Settings



## ▼ Erzeugen eines neuen Schlüssels mithilfe der CLI

1. **Legen Sie den Schlüsseltyp durch folgende Eingabe fest:**

   ```
   -> set /SP/services/ssh generate_new_key_type=dsa | rsa
   ```

2. **Legen Sie die Aktion auf** `true` **fest.**

   ```
   -> set /SP/services/ssh generate_new_key_action=true
   ```

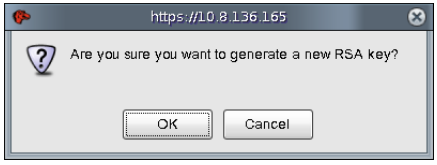
   Fingerabdruck und Schlüssel sehen unterschiedlich aus.

## ▼ Erzeugen eines neuen Schlüssels mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich bei ILOM als Administrator an.**
2. **Wählen Sie Configuration --> System Management Access --> SSH Server.**
3. **Wählen Sie RSA, indem Sie auf die Schaltfläche Generate RSA Key klicken, oder wählen Sie DSA, indem Sie auf die Schaltfläche Generate DSA Key klicken.**

   Bestätigen Sie die Auswahl durch Klicken auf OK, oder brechen Sie sie durch Klicken auf Cancel ab, wenn Sie dazu aufgefordert werden.

**ABBILDUNG 8-2** Bestätigungsdialogfeld




## ▼ Neustart des SSH-Servers mithilfe der CLI

Ein neuer Schlüssel wird erst gültig, nachdem der SSH-Server neu gestartet wurde.

---

**Hinweis –** Ein Neustart beendet alle bestehenden SSH-Verbindungen.

---

- **Geben Sie zum Neustarten des SSH-Servers Folgendes ein:**

  ```
  -> set /SP/services/ssh restart_sshd_action=true
  ```

## ▼ Neustart des SSH-Servers mithilfe der Webbenutzeroberfläche

Ein neuer Schlüssel wird erst gültig, nachdem der SSH-Server neu gestartet wurde.

---

**Hinweis –** Ein Neustart beendet alle bestehenden SSH-Verbindungen.

---

1. **Melden Sie sich bei ILOM als Administrator an.**
2. **Wählen Sie Configuration --> System Management Access --> SSH Server.**
3. **Wählen Sie im Dropdown-Listenfeld SSH Server den Eintrag Restart SSH Server.**

# Verwalten von ILOM-Netzwerkeinstellungen mithilfe der Webbenutzeroberfläche

In diesem Abschnitt wird beschrieben, wie die Netzwerkparameter für ILOM mithilfe der ILOM-Webbenutzeroberfläche konfiguriert werden.

ILOM konfiguriert seine IP-Einstellungen automatisch mithilfe von DHCP (Dynamic Host Configuration Protocol). Wenn dieses Protokoll von Ihrem Netzwerk nicht unterstützt wird, müssen Sie die Parameter manuell festlegen.

## ▼ Anzeigen von Netzwerkeinstellungen mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich bei ILOM als Administrator oder Operator an, um die ILOM-Webbenutzeroberfläche zu öffnen.**
2. **Wählen Sie Configuration --> Network.**

   Auf der Seite Network Settings können Sie MAC-Adressen anzeigen und Netzwerkadressen für die CMMs (Chassis Monitoring Module) und SPs (Service-Prozessor) des Servers konfigurieren.

---

**Hinweis –** DHCP ist zwar der Standardmodus, doch alle IP-Adressen, Netzmasken und Gateways können manuell konfiguriert werden.

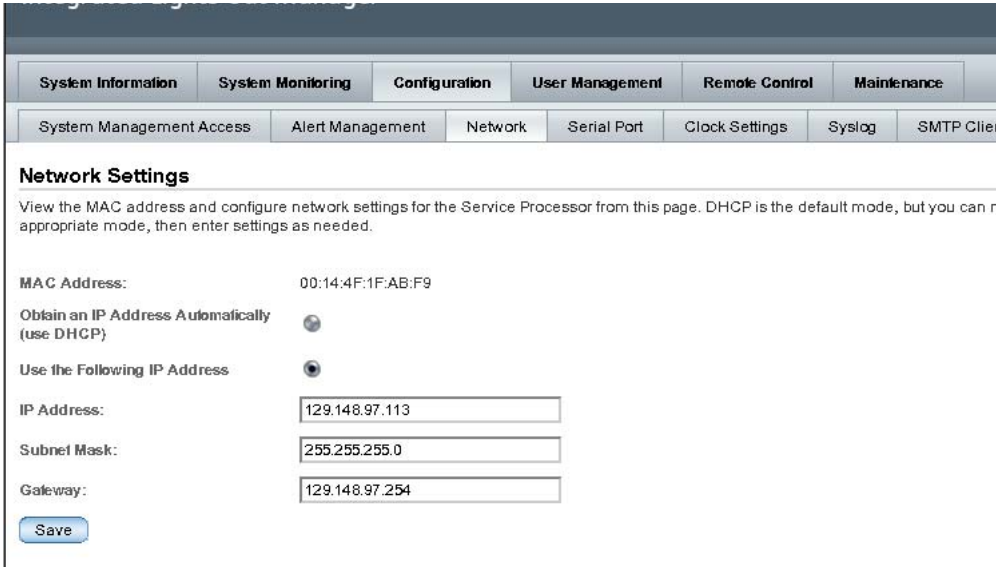
---

## ▼ Konfigurieren von Netzwerkeinstellungen mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich bei ILOM als Administrator an, um die ILOM-Webbenutzeroberfläche zu öffnen.**
2. **Wählen Sie Configuration --> Network.**

   Die Seite Network Settings wird angezeigt.

**ABBILDUNG 8-3** Seite Network Settings



3. **Tragen Sie die Informationen auf der Seite Network Settings ein.**

   Orientieren Sie sich hierbei an den Beschreibungen in TABELLE 8-5.

**TABELLE 8-5** Felder der Seite Network Settings

| Element | Beschreibung |
|---|---|
| MAC Address | Die MAC-Adresse (Media Access Control) von ILOM wird werkseitig festgelegt. Es handelt sich dabei um eine Hardwareadresse, die jedem Netzwerkgerät eindeutig zugeordnet ist. Die MAC-Adresse von ILOM finden Sie auf einem Etikett am Server oder CMM, auf dem Kundeninformationsblatt, das im Lieferumfang enthalten ist, sowie im Bildschirm zum Einrichten des BIOS. |
| Obtain an IP Address Automatically (use DHCP) | Klicken Sie auf das Optionsfeld, damit eine IP-Adresse von DHCP abgerufen wird. |
| IP Address | Geben Sie die IP-Adresse von ILOM ein. Die IP-Adresse ist ein eindeutiger Name, der das System in einem TCP/IP-Netzwerk eindeutig identifiziert. |
| Subnet Mask | Geben Sie die Teilnetzmaske des Netzwerks ein, in dem sich ILOM befindet. |
| Gateway | Geben Sie die Zugriffsadresse für das Gateway von ILOM ein. |

4. **Klicken Sie auf Save, um die neuen Einstellungen zu übernehmen.**

   Einstellungen werden als anstehend eingestuft, bis Sie auf Save klicken. Das Ändern der IP-Adresse beendet Ihre ILOM-Sitzung.

   Sie werden zum Schließen des Webbrowsers aufgefordert.

5. **Melden Sie sich erneut bei ILOM unter Verwendung der neuen IP-Adresse an.**

---

**Hinweis –** Wenn Sie die Netzwerkeinstellungen geändert haben, müssen Sie sich möglicherweise mit einer neuen Browsersitzung erneut anmelden.

---

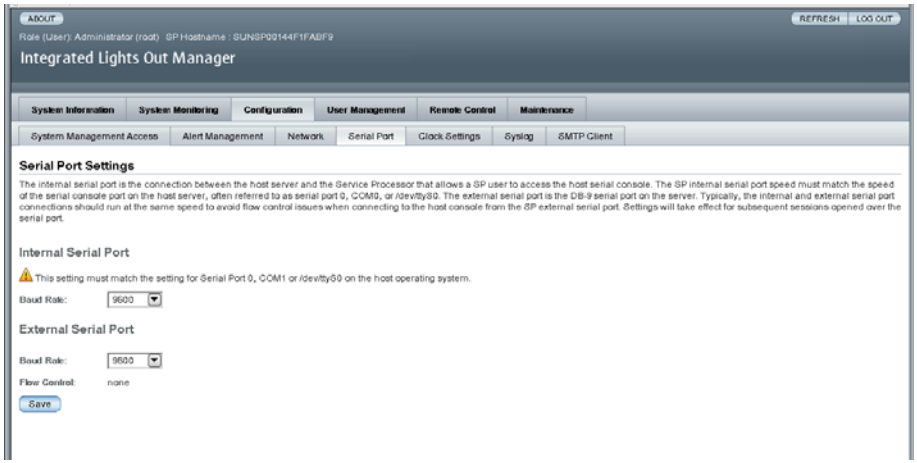
## ▼ Anzeigen von seriellen Anschlusseinstellungen mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich bei der ILOM-Webbenutzeroberfläche als Administrator oder Operator an.**

2. **Wählen Sie Configuration --> Serial Port.**

   Die Seite Serial Port Settings wird angezeigt.

**ABBILDUNG 8-4** Seite Serial Port Settings


ABOUT
REFRESH
LOG OUT
Role (User): Administrator (root) SP Hostname : SUNSP00144F1FABF9
Integrated Lights Out Manager
System Information
System Monitoring
Configuration
User Management
Remote Control
Maintenance
System Management Access
Alert Management
Network
Serial Port
Clock Settings
Syslog
SMTP Client
Serial Port Settings
The internal serial port is the connection between the host server and the Service Processor that allows a SP user to access the host serial console. The SP internal serial port speed must match the speed of the serial console port on the host server, often referred to as serial port 0, COM0, or /dev/ttyS0. The external serial port is the DB-9 serial port on the server. Typically, the internal and external serial port connections should run at the same speed to avoid flow control issues when connecting to the host console from the SP external serial port. Settings will take effect for subsequent sessions opened over the serial port.
Internal Serial Port
This setting must match the setting for Serial Port 0, COM1 or /dev/ttyS0 on the host operating system.
Baud Rate:
9600
External Serial Port
Baud Rate:
9600
Flow Control:
none
Save

3. **Zeigen Sie die Baudrate für den externen seriellen Anschluss an.**

## ▼ Konfigurieren von seriellen Anschlusseinstellungen mithilfe der Webbenutzeroberfläche

In diesem Abschnitt wird beschrieben, wie der serielle ILOM-Anschluss konfiguriert wird. Die Standardeinstellungen sind 9600 Baud und keine Flusssteuerung.

1. **Melden Sie sich bei ILOM als Administrator an, um die ILOM-Webbenutzeroberfläche zu öffnen.**
2. **Wählen Sie Configuration --> Serial Port.**

   Die Seite Serial Port Settings wird angezeigt.

3. **Wählen Sie in dem Dropdown-Listenfeld Internal Serial Port Baud Rate die Baudrate für den internen seriellen Anschluss aus.**

   Diese Einstellung muss mit der Einstellung für den seriellen Anschluss 0, COM1 oder /dev/ttyS0 des Hostbetriebssystems übereinstimmen.

   Der Baudratenwert muss mit der Geschwindigkeit übereinstimmen, die für die serielle Umleitungsfunktion des BIOS angegeben wurde (Standardwert ist 9600 Baud), und mit der für den Bootloader und die Betriebssystemkonfiguration verwendeten Geschwindigkeit.

   Zum Herstellen einer Verbindung mit der Systemkonsole mithilfe von ILOM muss ILOM auf seine Standardeinstellungen festgelegt sein (9600 Baud, 8N1 [acht Daten-Bits, keine Parität, ein Stopp-Bit], keine Flusssteuerung).

4. **Wählen Sie in dem Dropdown-Listenfeld External Serial Port Baud Rate die Baudrate für den externen seriellen Anschluss aus.**

   Diese Einstellung muss mit der Baudrate des seriellen RJ-45-Anschlusses am Server übereinstimmen.

5. **Klicken Sie auf Save, um die Änderungen zu übernehmen, oder klicken Sie auf Cancel, um zu den vorherigen Einstellungen zurückzukehren.**

## ▼ Aktivieren von HTTP- oder HTTPS-Webzugriff mithilfe der Webbenutzeroberfläche

In diesem Abschnitt wird beschrieben, wie Webservereinstellungen angezeigt und geändert werden.

ILOM bietet die Möglichkeit, den Zugriff auf die Webbenutzeroberfläche zu steuern. Es gibt vier Optionen:

- Nur HTTP
- Nur HTTPS
- HTTP und HTTPS
- HTTPS und automatische Umleitung von HTTP auf HTTPS

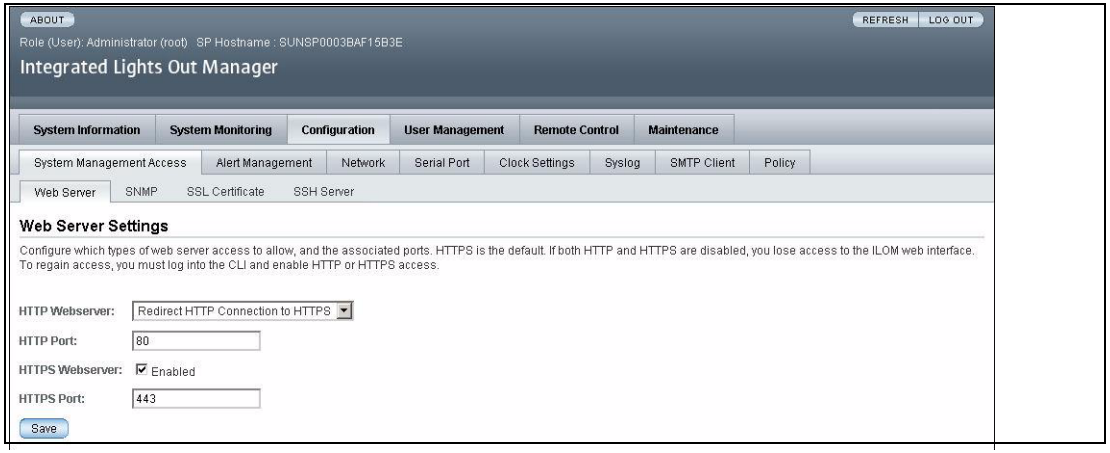
HTTPS ist standardmäßig aktiviert.

1. **Melden Sie sich bei ILOM als Administrator an, um die ILOM-Webbenutzeroberfläche zu öffnen.**

2. **Wählen Sie Configuration --> System Management Access --> Web Server.**

   Die Seite Web Server Settings wird angezeigt.

**ABBILDUNG 8-5** Seite Web Server Settings




3. **Wählen Sie den HTTP- oder HTTPS-Webserver aus.**
   - **Aktivieren von HTTP** – Wählen Sie im Dropdown-Listenfeld den Eintrag Enabled aus. Sie können auch Folgendes wählen:
     - Redirect HTTP Connection to HTTPS – HTTP-Verbindungen werden automatisch auf HTTPS umgeleitet.
     - Disabled – Deaktiviert HTTP.
   - **Aktivieren von HTTPS** – Aktivieren Sie das Kontrollkästchen HTTPS Web Server Enabled.

   Der HTTPS-Webserver ist standardmäßig aktiviert.

---

**Hinweis –** Wenn Sie HTTP deaktivieren oder Redirect HTTP Connection to HTTPS wählen und dann HTTPS deaktivieren, ist kein Zugriff mehr auf die ILOM-Webbenutzeroberfläche möglich. Um den Zugriff wieder zu ermöglichen, verwenden Sie die CLI-Befehle `/SP/services/http` oder `/SP/services/https` wie unter „Aktivieren von HTTP- oder HTTPS-Webzugriff mithilfe der CLI“ auf Seite 164 beschrieben.

---

4. **Weisen Sie eine HTTP- oder HTTPS-Anschlussnummer zu.**
5. **Klicken Sie auf Save, um die neuen Einstellungen zu übernehmen.**

KAPITEL 9

# Intelligent Platform Management Interface (IPMI)

ILOM unterstützt die Intelligente Plattformverwaltungsschnittstelle (Intelligent Platform Management Interface, IPMI), mit der unter Verwendung einer Befehlszeilenschnittstelle die Serverplattform überwacht und gesteuert sowie Informationen zur Serverplattform abgerufen werden können.

Dieses Kapitel enthält folgende Abschnitte:


- „IPMI – Überblick“ auf Seite 177
- „ILOM und IPMI“ auf Seite 178
- „Verwenden von IPMItool“ auf Seite 178
- „IPMI-Alarme“ auf Seite 179
- „IPMItool-Beispiele“ auf Seite 180


## IPMI – Überblick

IPMI (Intelligent Platform Management Interface) ist eine Schnittstelle gemäß offenem Industriestandard, die primär für die Out-of-Band-Verwaltung von Serversystemen über eine Reihe von verschiedenen Typen von Netzwerken entwickelt wurde. Die IPMI-Funktionalität umfasst die Erstellung von FRU-Bestandsberichten (Field Replacable Unit), Systemüberwachung, Protokollierung von Systemereignissen, Systemwiederherstellung (einschließlich lokalem und entferntem Zurücksetzen des Systems sowie Ein- und Ausschaltfunktionen) und Alarme. IPMI arbeitet unabhängig vom Hauptprozessor und dem Betriebssystem.

Die über IPMI verfügbaren unabhängigen Überwachungs-, Protokollier- und Zugriffsfunktionen bieten ein gewisses Maß an Verwaltungsmöglichkeiten, die in die Plattformhardware integriert sind. IPMI unterstützt außerdem Systeme, bei denen für ein bestimmtes Betriebssystem keine Systemverwaltungssoftware verfügbar ist, bzw. wenn die Systemverwaltungssoftware nicht installiert oder geladen werden soll.

ILOM ist kompatibel mit IPMI v1.5 und v2.0.

Zusätzliche Informationen, einschließlich detaillierter Spezifikationen über IPMI, finden Sie auf den folgenden Sites:

`http://www.intel.com/design/servers/ipmi/spec.htm`

`http://openipmi.sourceforge.net`

# ILOM und IPMI

IPMI definiert eine spezielle Methode für die Kommunikation eingebetteter Verwaltungssubsysteme. IPMI-Informationen werden über Baseboard Management Controller (BMC) ausgetauscht, die sich auf IPMI-kompatiblen Hardwarekomponenten befinden. Die Verwendung von hardwarenaher Technologie anstelle des Betriebssystems hat zwei Hauptvorteile: Erstens ermöglicht diese Konfiguration die Out-of-Band-Serververwaltung, und zweitens wird das Betriebssystem nicht mit Statusdaten des Transportsystems belastet.

Die auf Ihrem Server oder Blades vorhandenen Service-Prozessoren (SPs) sind IPMI v2.0-kompatibel. Der Zugriff auf die IPMI-Funktionalität kann über die Befehlszeile unter Verwendung des Dienstprogramms „IPMItool“ entweder In-Band oder Out-of-Band erfolgen. Darüber hinaus können Sie über die ILOM-Webbenutzeroberfläche IPMI-spezifische Traps erzeugen oder die IPMI-Funktionen des SP über eine beliebige externe Verwaltungslösung, die mit IPMI v1.5 oder v2.0 kompatibel ist, verwalten.

# Verwenden von IPMItool

IPMItool ist ein einfaches Open Source-Befehlszeilen-Dienstprogramm (Command-Line Interface, CLI) zum Verwalten und Konfigurieren IPMI-fähiger Geräte. Mit IPMItool können IPMI-Funktionen des lokalen Systems oder eines entfernten Systems verwaltet werden. Mithilfe des IPMItool-Dienstprogramms können Sie IPMI-Funktionen mit einem Kernel-Gerätetreiber oder über eine LAN-Schnittstelle ausführen. IPMItool kann von folgender Site heruntergeladen werden:

`http://ipmitool.sourceforge.net/`

Sie können folgende Aktionen mit IPMItool ausführen:

- Lesen des SDR-Repositorys (Sensor Data Record, Sensordatensatz)
- Drucken von Sensorwerten
- Anzeigen des Inhalts des Systemereignisprotokolls (SEL)

- Drucken von FRU-Bestandsinformationen (Field Replaceable Unit)
- Lesen und Festlegen von LAN-Konfigurationsparametern
- Entfernte Steuerung der Gehäusestromversorgung

Ausführliche Informationen zu IPMItool finden Sie auf der Man Page, die auf folgender Site verfügbar ist:

`http://ipmitool.sourceforge.net/manpage.html`

# IPMI-Alarme

ILOM unterstützt Alarme in der Form von IPMI PET-Alarmen (Platform Event Trap, Plattformereignis-Trap). Alarme bieten Vorabwarnungen bei möglichen Systemfehlern. Die Alarmkonfiguration erfolgt über den SP auf Ihrem Server oder Blade. IPMI PET-Alarme werden auf allen Serverplattformen und Modulen unterstützt, mit Ausnahme des Chassis Monitoring Module (CMM).

Jede Serverplattformen ist mit einer Anzahl von IPMI-kompatiblen Sensoren ausgestattet, die Spannungen, Temperaturen und andere betriebsbezogene Attribute des Systems messen. ILOM ruft diese Sensoren automatisch ab und erfasst alle Ereignisse, die einen Schwellenwert überschreiten, in einem ILOM-Ereignisprotokoll. Zusätzlich erzeugt ILOM Alarmmeldungen an ein oder mehrere Alarmziele, die von Ihnen mit IP-Adresse angegeben werden. Das angegebene Alarmziel muss das Empfangen von IPMI PET-Meldungen unterstützen. Unterstützt das Alarmziel den Empfang von IPMI PET-Meldungen nicht, kann der Alarmempfänger die Alarmmeldung nicht dekodieren.

Beim Konfigurieren von IPMI PET-Alarmen müssen Sie ebenfalls eine Alarmstufe angeben, anhand der Alarmmeldungen so gefiltert werden, dass Alarmempfänger nur solche Meldungen erhalten, an deren Erhalt sie vornehmlich interessiert sind. ILOM stellt fünf Alarmstufen bereit, wobei Minor (Geringfügig) die niedrigste ist:

- **Minor** – Erzeugt Alarme für Informationsereignisse, nicht kritische obere und untere Schwellenwertereignisse, kritische obere und untere Schwellenwertereignisse sowie nicht wiederherstellbare obere und untere Schwellenwertereignisse.
- **Major** – Erzeugt Alarme für nicht kritische obere und untere Schwellenwertereignisse, kritische obere und untere Schwellenwertereignisse sowie nicht wiederherstellbare obere und untere Schwellenwertereignisse.
- **Critical** – Erzeugt Alarme für kritische obere und untere Schwellenwertereignisse sowie nicht wiederherstellbare obere und untere Schwellenwertereignisse.
- **Down** – Erzeugt nur Alarme für nicht wiederherstellbare obere und untere Schwellenwertereignisse.
- **Disabled** – Deaktiviert den Alarm. ILOM erzeugt dann keine Alarmmeldung.

Informationen zum Verwalten von Alarmregelkonfigurationen, einschließlich des Änderns und Deaktivierens einer Alarmregel sowie des Erzeugens eines Testalarms, finden Sie unter „Verwalten von Alarmregelkonfigurationen mithilfe der ILOM-Webbenutzeroberfläche“ auf Seite 145 und „Verwalten von Alarmregelkonfigurationen mithilfe der ILOM-CLI“ auf Seite 149.

Eine Beschreibung der ILOM-CLI-Befehle zum Verwalten von Alarmregelkonfigurationen finden Sie unter „CLI-Befehle zum Verwalten von Alarmregelkonfigurationen“ auf Seite 150.

# IPMItool-Beispiele

Im Folgenden finden Sie Beispiele für die Verwendung von IPMItool. In den Beispielen wird „10.8.136.165“ als IP-Adresse von ILOM verwendet. Die Befehle stehen auf allen Plattformen zur Verfügung. Die Ausgabe (Sensornamen, Werte, Schwellenwerte usw.) ist aber plattformspezifisch.

## ▼ Anzeigen einer Liste von Sensoren mit ihren Werten

```
$ ipmitool -H 10.8.136.165 -I lanplus -U root -P changeme sdr list
/SYS/T_AMB       | 24 degrees C       | ok
/RFM0/FAN1_SPEED | 7110 RPM           | ok
/RFM0/FAN2_SPEED | 5880 RPM           | ok
/RFM1/FAN1_SPEED | 5880 RPM           | ok
/RFM1/FAN2_SPEED | 6360 RPM           | ok
/RFM2/FAN1_SPEED | 5610 RPM           | ok
/RFM2/FAN2_SPEED | 6510 RPM           | ok
/RFM3/FAN1_SPEED | 6000 RPM           | ok
/RFM3/FAN2_SPEED | 7110 RPM           | ok
/RFM4/FAN1_SPEED | 6360 RPM           | ok
/RFM4/FAN2_SPEED | 5610 RPM           | ok
/RFM5/FAN1_SPEED | 5640 RPM           | ok
/RFM5/FAN2_SPEED | 6510 RPM           | ok
/RFM6/FAN1_SPEED | 6180 RPM           | ok
/RFM6/FAN2_SPEED | 6000 RPM           | ok
/RFM7/FAN1_SPEED | 6330 RPM           | ok
/RFM7/FAN2_SPEED | 6330 RPM           | ok
/RFM8/FAN1_SPEED | 6510 RPM           | ok
/RFM8/FAN2_SPEED | 5610 RPM           | ok
```

**Hinweis –** Die vorangehende Ausgabe wurde gekürzt. In der tatsächlichen Ausgabe werden 163 Sensoren angezeigt.

### ▼ Anzeigen von Detailinformationen zu einem einzelnen Sensor

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme sensor get /SYS/T_AMB
Locating sensor record...
Sensor ID              : /SYS/T_AMB (0x8)
 Entity ID             : 41.0
 Sensor Type (Analog)  : Temperature
 Sensor Reading        : 24 (+/- 0) degrees C
 Status                : ok
 Lower Non-Recoverable : 0.000
 Lower Critical        : 4.000
 Lower Non-Critical    : 10.000
 Upper Non-Critical    : 35.000
 Upper Critical        : 40.000
 Upper Non-Recoverable : 45.000
 Assertions Enabled    : lnc- lcr- lnr- unc+ ucr+ unr+
 Deassertions Enabled  : lnc- lcr- lnr- unc+ ucr+ unr+
```

### ▼ Einschalten des Systems

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme chassis
power on
```

### ▼ Ausschalten des Systems

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme chassis
power off
```

### ▼ Aus- und Wiedereinschalten des Systems (Power Cycle)

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme chassis
power cycle
```

### ▼ Ordnungsgemäßes Herunterfahren des Hosts

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme chassis
power soft
```

## ▼ Anzeigen von Herstellerinformationen für FRUs

```
$ ipmitool -H 10.8.136.165 -v -I lanplus -U root -P changeme fru print
FRU Device Description : Builtin FRU Device (ID 0)
 Board Product         : ASSY,ANDY,4SKT_PCI-E,BLADE
 Board Serial          : 0000000-7001
 Board Part Number     : 501-7738-01
 Board Extra           : AXX_RevE_Blade
 Product Manufacturer  : SUN MICROSYSTEMS
 Product Name          : ILOM

FRU Device Description : /SYS (ID 4)
 Chassis Type          : Rack Mount Chassis
 Chassis Part Number   : 541-0251-05
 Chassis Serial        : 00:03:BA:CD:59:6F
 Board Product         : ASSY,ANDY,4SKT_PCI-E,BLADE
 Board Serial          : 0000000-7001
 Board Part Number     : 501-7738-01
 Board Extra           : AXX_RevE_Blade
 Product Manufacturer  : SUN MICROSYSTEMS
 Product Name          : SUN BLADE X8400 SERVER MODULE
 Product Part Number   : 602-0000-00
 Product Serial        : 0000000000
 Product Extra         : 080020ffffffffffffff0003baf15c5a

FRU Device Description : /P0 (ID 5)
 Product Manufacturer  : ADVANCED MICRO DEVICES
 Product Part Number   : 0F21
 Product Version       : 2

FRU Device Description : /P0/D0 (ID 6)
 Product Manufacturer  : MICRON TECHNOLOGY
 Product Name          : 1024MB DDR 400 (PC3200) ECC
 Product Part Number   : 18VDDF12872Y-40BD3
 Product Version       : 0300
 Product Serial        : D50209DA
 Product Extra         : 0190
 Product Extra         : 0400

FRU Device Description : /P0/D1 (ID 7)
 Product Manufacturer  : MICRON TECHNOLOGY
 Product Name          : 1024MB DDR 400 (PC3200) ECC
 Product Part Number   : 18VDDF12872Y-40BD3
 Product Version       : 0300
 Product Serial        : D50209DE
 Product Extra         : 0190
 Product Extra         : 0400
```

## ▼ Anzeigen des IPMI-Systemereignisprotokolls (SEL)

```
$ ipmitool -H 10.8.136.165 -I lanplus -U root -P changeme sel list
 100 | Pre-Init Time-stamp   | Power Unit #0x78 | State Deasserted
 200 | Pre-Init Time-stamp   | Power Supply #0xa2 | Predictive Failure Asserted
 300 | Pre-Init Time-stamp   | Power Supply #0xba | Predictive Failure Asserted
 400 | Pre-Init Time-stamp   | Power Supply #0xc0 | Predictive Failure Asserted
 500 | Pre-Init Time-stamp   | Power Supply #0xb4 | Predictive Failure Asserted
 600 | 04/05/2007 | 12:03:24 | Power Supply #0xa3 | Predictive Failure Deasserted
 700 | 04/05/2007 | 12:03:25 | Power Supply #0xaa | Predictive Failure Deasserted
 800 | 04/05/2007 | 12:03:25 | Power Supply #0xbc | Predictive Failure Deasserted
 900 | 04/05/2007 | 12:03:26 | Power Supply #0xa2 | Predictive Failure Asserted
 a00 | 04/05/2007 | 12:03:26 | Power Supply #0xa8 | Predictive Failure Deasserted
 b00 | 04/05/2007 | 12:03:26 | Power Supply #0xb6 | Predictive Failure Deasserted
 c00 | 04/05/2007 | 12:03:26 | Power Supply #0xbb | Predictive Failure Deasserted
 d00 | 04/05/2007 | 12:03:26 | Power Supply #0xc2 | Predictive Failure Deasserted
 e00 | 04/05/2007 | 12:03:27 | Power Supply #0xb0 | Predictive Failure Deasserted
 f00 | 04/05/2007 | 12:03:27 | Power Supply #0xb5 | Predictive Failure Deasserted
1000 | 04/05/2007 | 12:03:27 | Power Supply #0xba | Predictive Failure Asserted
1100 | 04/05/2007 | 12:03:27 | Power Supply #0xc0 | Predictive Failure Asserted
1200 | 04/05/2007 | 12:03:28 | Power Supply #0xa9 | Predictive Failure Deasserted
1300 | 04/05/2007 | 12:03:28 | Power Supply #0xae | Predictive Failure Deasserted
1400 | 04/05/2007 | 12:03:28 | Power Supply #0xb4 | Predictive Failure Asserted
1500 | 04/05/2007 | 12:03:28 | Power Supply #0xbe | Predictive Failure Deasserted
```

KAPITEL 10

# SNMP (Simple Network Management Protocol)

ILOM unterstützt SNMP (Simple Network Management Protocol), das für den Austausch von Daten über die Netzwerkaktivität verwendet wird. SNMP ist ein offenes Industriestandardprotokoll.

Dieses Kapitel enthält folgende Abschnitte:


- „SNMP – Überblick“ auf Seite 186
- „Funktionsweise von SNMP“ auf Seite 187
- „Grundlegende Dateien mit SNMP-Verwaltungsinformationen“ auf Seite 188
- „Alarme und SNMP-Traps“ auf Seite 189
- „Verwalten von SNMP mithilfe der CLI“ auf Seite 189
  - „Hinzufügen eines SNMP-Benutzerkontos mithilfe der CLI“ auf Seite 190
  - „Bearbeiten eines SNMP-Benutzerkontos mithilfe der CLI“ auf Seite 190
  - „Löschen eines SNMP-Benutzerkontos mithilfe der CLI“ auf Seite 190
  - „Hinzufügen oder Bearbeiten einer SNMP-Community mithilfe der CLI“ auf Seite 190
  - „Löschen einer SNMP-Community mithilfe der CLI“ auf Seite 191
  - „Konfigurieren von SNMP-Trap-Zielen mithilfe der CLI“ auf Seite 192
- „Verwalten von SNMP-Benutzern mithilfe der Webbenutzeroberfläche“ auf Seite 193
  - „Konfigurieren von SNMP-Einstellungen mithilfe der Webbenutzeroberfläche“ auf Seite 193
  - „Hinzufügen oder Bearbeiten eines SNMP-Benutzerkontos mithilfe der Webbenutzeroberfläche“ auf Seite 194
  - „Löschen eines SNMP-Benutzerkontos mithilfe der Webbenutzeroberfläche“ auf Seite 196

- „Hinzufügen oder Bearbeiten einer SNMP-Community mithilfe der Webbenutzeroberfläche“ auf Seite 196
- „Löschen einer SNMP-Community mithilfe der Webbenutzeroberfläche“ auf Seite 197
- „Konfigurieren von SNMP-Trap-Zielen mithilfe der Webbenutzeroberfläche“ auf Seite 198

- „SNMP-Beispiele“ auf Seite 198
  - „Anzeigen und Konfigurieren von SNMP-Einstellungen“ auf Seite 199
  - „Abrufen von Informationen mithilfe der Befehl `snmpget` oder `snmpwalk net-snmp`“ auf Seite 200
  - „Festlegen von Informationen mithilfe von `snmpset`“ auf Seite 201
  - „Empfangen von Traps mithilfe von `snmptrapd`“ auf Seite 201


---

**Hinweis –** In diesem Kapitel verwendete Syntaxbeispiele verwenden das Ziel beginnend mit `/SP/`. Dies könnte in Abhängigkeit von der verwendeten Serverplattform gegen das Ziel beginnend mit `/CMM/` ausgetauscht werden. Unterziele sind auf allen Serverplattformen gleich.

---

# SNMP – Überblick

SNMP ist eine offene Technologie, die die Verwaltung von Netzwerken und Geräten bzw. Knoten ermöglicht, die an das Netzwerk angeschlossen sind. Mithilfe von SNMP werden Daten zwischen einem verwalteten Gerät (Knoten) und einer Station zur Netzwerkverwaltung übertragen. Bei dem verwalteten Gerät kann es sich um ein beliebiges Gerät handeln, das SNMP ausführt, wie z. B. Hosts, Router, Webserver oder andere Server im Netzwerk. SNMP-Meldungen werden über IP mithilfe von UDP (User Datagram Protocol) gesendet. Ihr Server kann mit jeder Anwendung, die SNMP unterstützt, verwaltet werden.

ILOM unterstützt die SNMP-Versionen 1, 2c und 3. Es wird dringend empfohlen, SNMP v3 zu verwenden, weil SNMP v3 zusätzliche Sicherheit, Authentifizierung und Datenschutz gegenüber SNMP v1 und v2c bietet.

SNMP ist ein Protokoll und kein Betriebssystem, weshalb Sie zur Verwendung von SNMP-Meldungen eine Anwendung benötigen. Die verwendete SNMP-Verwaltungssoftware kann diese Funktion bereitstellen, oder Sie können ein Open Source-Tool wie „net-SNMP“ verwenden, das verfügbar ist unter:

`http://net-snmp.sourceforge.net/`

Sowohl Verwaltungsstationen als auch -agenten verwenden zur Kommunikation SNMP-Meldungen. Verwaltungsstationen können Informationen senden und empfangen. Agenten können auf Anforderungen antworten und unaufgeforderte Meldungen in Form von Traps senden. Verwaltungsstationen und -agenten verwenden folgende Funktionen:

- Get
- GetNext
- GetResponse
- Set
- Trap

# Funktionsweise von SNMP

Die SNMP-Funktion erfordert die beiden folgenden Komponenten:

- **Station zur Netzwerkverwaltung** – Eine Station zur Netzwerkverwaltung (Network Management Station, NMS) enthält Verwaltungsanwendungen, mit denen verwaltete Knoten überwacht und gesteuert werden.
- **Verwalteter Knoten** – Ein verwalteter Knoten ist ein Gerät, wie z. B. ein Server, Router oder Hub, auf dem sich SNMP-Verwaltungsagenten befinden, die für das Ausführen von Anforderungen von Verwaltungsstationen, wie z. B. einem SP, auf dem ILOM ausgeführt wird, verantwortlich sind.

Die Verwaltungsstation überwacht Knoten, indem sie mithilfe von Abfragen die geeigneten Informationen von Verwaltungsagenten abruft. Verwaltete Knoten können einer Verwaltungsstation außerdem unaufgeforderte Statusinformationen in Form einer Trap bieten. SNMP ist das Protokoll, das für die Übermittlung von Verwaltungsinformationen zwischen Verwaltungsstationen und -agenten verwendet wird.

Der SNMP-Agent ist auf Ihrer Serverplattform vorinstalliert und wird auf ILOM ausgeführt, sodass die gesamte SNMP-Verwaltung über ILOM erfolgt. Um dieses Leistungsmerkmal einzusetzen, muss Ihr Betriebssystem über eine SNMP-Clientanwendung verfügen.

# Grundlegende Dateien mit SNMP-Verwaltungsinformationen

Dies Basiskomponente einer SNMP-Implementierung ist die Verwaltungsinformationsbasis (Management Information Base, MIB). Eine MIB ist eine Textdatei, die die für einen verwalteten Knoten verfügbaren Informationen sowie deren Speicherort beschreibt. Das baumartig strukturierte, hierarchische System klassifiziert Informationen über Ressourcen in einem Netzwerk. In der MIB sind die Variablen definiert, auf die der SNMP-Agent zugreifen kann. Wenn eine Verwaltungsstation Informationen von einem verwalteten Knoten anfordert, empfängt der Agent die Anforderung und ruft die entsprechenden Informationen in den MIBs ab. Die MIB bietet Zugriff auf die Netzwerkkonfiguration, den Status und Statistiken des Servers.

Folgende SNMP-MIBs werden mit ILOM verwendet:

- Die System- und SNMP-Gruppen der SNMPv2 MIB (RFC 1907)
- SNMP-FRAMEWORK-MIB (RFC2271.txt)
- SNMP-USER-BASED-MIB (RFC 2574)
- SNMP-MPD-MIB (RFC 2572)
- Die entPhysicalTable der ENTITY-MIB (RFC 2737)
- SUN-PLATFORM-MIB

  Diese MIB stellt ein Bestandsverzeichnis der Server- und Gehäusehardware dar, einschließlich aller Sensoren und LEDs zusammen mit deren Status.

- SUN-ILOM-CONTROL-MIB

  Diese MIB stellt eine SP- oder CMM-Konfiguration dar wie Benutzer- oder Zugriffsverwaltung, Alarme und mehr.

- SUN-HW-TRAP-MIB

  Diese MIB beschreibt die hardwarebezogenen Traps, die von einem SP oder CMM erzeugt werden können.

- SUN-ILOM-PET-MIB

  Diese MIB beschreibt die IPMI PETs (Platform Event Trap), die von einem SP erzeugt werden können. Weitere Informationen zu PETs finden Sie unter „Informationen zur Alarmverwaltung“ auf Seite 141.

# Alarme und SNMP-Traps

Mit ILOM können bis zu 15 Alarmregeln konfiguriert werden. Für jede in ILOM konfigurierte Alarmregel müssen in Abhängigkeit vom Alarmtyp mindestens drei Alarmeigenschaften definiert werden. Der Alarmtyp definiert das Meldungsformat sowie die Methode zum Senden und Empfangen einer Alarmmeldung. ILOM unterstützt die folgenden drei Alarmtypen: IPMI PET-Alarme, E-Mail-Benachrichtigungsalarme und SNMP-Traps.

ILOM unterstützt die Erzeugung von SNMP-Trap-Alarmen und das Versenden an eine individuell angegebene IP-Adresse. Alle angegebenen Ziele müssen das Empfangen von SNMP-Trap-Meldungen unterstützen.

ILOM verfügt über einen vorinstallierten SNMP-Agent, der die SNMP-Trap-Zustellung an eine SNMP-Verwaltungsanwendung unterstützt.

Gehen Sie zur Verwendung dieses Leistungsmerkmals wie folgt vor:

- Integrieren und speichern Sie die plattformspezifischen MIBs in Ihrem SNMP-Verzeichnis.
- Informieren Sie die Verwaltungsstation über den Server.
- Konfigurieren Sie ILOM für das Senden von SNMP-Traps an Ihre Verwaltungsstation.

Standardmäßig sind keine Trap-Ziele konfiguriert. Agenten überwachen standardmäßig Anschluss 161 auf SNMP-Anforderungen und senden Traps an Anschluss 162.

# Verwalten von SNMP mithilfe der CLI

Sie können mithilfe der ILOM-CLI SNMP-Benutzerkonten und -Communitys hinzufügen, löschen und konfigurieren.

---

**Hinweis –** Wenn bei der Arbeit in der ILOM-CLI Set Requests deaktiviert ist, sind alle SNMP-Objekte schreibgeschützt.

---

## ▼ Hinzufügen eines SNMP-Benutzerkontos mithilfe der CLI

1. **Melden Sie sich bei der ILOM-CLI als Administrator an.**
2. **Geben Sie zum Hinzufügen eines schreibgeschützten SNMP v3-Benutzerkontos folgenden Befehl ein:**

**`create /SP/services/snmp/users/`***Benutzername* **`authenticationpassword=`***Passwort*

## ▼ Bearbeiten eines SNMP-Benutzerkontos mithilfe der CLI

1. **Melden Sie sich bei der ILOM-CLI als Administrator an.**
2. **Geben Sie zum Bearbeiten eines SNMP v3-Benutzerkontos folgenden Befehl ein:**

**`edit /SP/services/snmp/users/`***Benutzername* **`authenticationpassword=`***Passwort*

---

**Hinweis –** Beim Ändern der Parameter von SNMP-Benutzern müssen Sie einen Wert für `authenticationpassword` angeben, auch wenn das Passwort nicht geändert wird.

---

## ▼ Löschen eines SNMP-Benutzerkontos mithilfe der CLI

1. **Melden Sie sich bei der ILOM-CLI als Administrator an.**
2. **Geben Sie zum Löschen eines SNMP v3-Benutzerkontos folgenden Befehl ein:**
   **`delete /SP/services/snmp/users/`***Benutzername*

## ▼ Hinzufügen oder Bearbeiten einer SNMP-Community mithilfe der CLI

1. **Melden Sie sich bei der ILOM-CLI als Administrator an.**
2. **Geben Sie zum Hinzufügen einer SNMP v1/v2-Community folgenden Befehl ein:**
   **`create /SP/services/snmp/communities/`***communityname*

## ▼ Löschen einer SNMP-Community mithilfe der CLI

1. **Melden Sie sich bei der ILOM-CLI als Administrator an.**
2. **Geben Sie zum Löschen einer SNMP v1/v2-Community folgenden Befehl ein:**
   **`delete /SP/services/snmp/communities/`***communityname*

# Ziele, Eigenschaften und Werte

In der folgenden Tabelle werden die Ziele, Eigenschaften und Werte aufgeführt, die für SNMP-Benutzerkonten gültig sind.

**TABELLE 10-1** Ziele, Eigenschaften und Werte von SNMP-Benutzerkonten

| Ziel | Eigenschaft | Wert | Standard |
|---|---|---|---|
| `/SP/services/snmp/communities/`*communityname* | `permissions` | `ro\|rw` | `ro` |
| `/SP/services/snmp/users/`*Benutzername* | `authenticationprotocol` | `MD5\|SHA` | `MD5` |
| | `authenticationpassword*` | <*Zeichenfolge*> | (leere Zeichenfolge) |
| | `permissions` | `ro\|rw` | `ro` |
| | `privacyprotocol` | `none\|DES` | `none` |
| | `privacypassword*` | <*Zeichenfolge*> | (leere Zeichenfolge) |
| `/SP/services/snmp` | `engineid = none` | <*Zeichenfolge*> | (leere Zeichenfolge) |
| | `port = 161` | <*Ganzzahl*> | `161` |
| | `sets = enabled` | `enabled\|disabled` | `disabled` |
| | `v1 = disabled` | `enabled\|disabled` | `disabled` |
| | `v2c = disabled` | `enabled\|disabled` | `disabled` |
| | `v3 = disabled` | `enabled\|disabled` | `enabled` |

* Wenn die Eigenschaft `privacyprotocol` einen anderen Wert als `none` hat, muss ein `privacypassword` festgelegt sein.
Ein `authenticationpassword` muss beim Erstellen oder Ändern von Benutzern angegeben werden (nur SNMP v3).

Um beispielsweise das `privacyprotocol` für den Benutzer `a1` in `DES` zu ändern, würden Sie Folgendes eingeben:

`->` **`set /SP/services/snmp/users/al privacyprotocol=DES privacypassword=`***Passwort* **`authenticationprotocol=SHA authenticationpassword=`***Passwort*

Wenn Sie nur Folgendes eingäben, wären die Änderungen ungültig:

`->` **`set /SP/services/snmp/users/al privacyprotocol=DES`**

**Hinweis –** SNMP-Benutzerberechtigungen können ohne Zurücksetzen der Datenschutz- und Authentifizierungseigenschaften geändert werden.

## ▼ Konfigurieren von SNMP-Trap-Zielen mithilfe der CLI

Führen Sie diese Schritte durch, um die Ziele zu konfigurieren, an die die SNMP-Traps gesendet werden.

1. **Melden Sie sich bei der ILOM-CLI als Administrator an.**
2. **Geben Sie den Befehl** `show` **ein, um die aktuellen Einstellungen der Alarmregel anzuzeigen.**

   Beispiel:

```
-> show
/SP/alertmgmt/rules/1
   Targets:
   Properties:
      community_or_username = public
      destination = 0.0.0.0
      level = disable
      snmp_version = 1
      type = snmptrap
   Commands:
     cd
     set
     show
```

3. **Wechseln Sie in das Verzeichnis** `/SP/alertmgmt/rules/snmp`**. Geben Sie Folgendes ein:**

   -> **cd /SP/alertmgmt/rules/snmp**

4. **Wählen Sie eine Regel (aus den Zielen 1 bis 15) aus, für die ein Ziel für SNMP-Traps konfiguriert werden soll, und wechseln Sie in dieses Verzeichnis.**

   Beispiel:

   -> **cd 4**

5. **Geben Sie in diesem Regelverzeichnis den Befehl** `set` **ein, um die Regeleigenschaften zu ändern.**

   Beispiel:

   -> **set type=snmptrap level=critical destination=***IPadresse* **snmp_version=2c community_or_username=public**

# Verwalten von SNMP-Benutzern mithilfe der Webbenutzeroberfläche

In diesem Abschnitt wird beschrieben, wie SNMP-Benutzer und -Communitys mithilfe der ILOM-Webbenutzeroberfläche verwaltet werden.

## ▼ Konfigurieren von SNMP-Einstellungen mithilfe der Webbenutzeroberfläche

Führen Sie diese Schritte durch, um SNMP-Einstellungen zu konfigurieren:

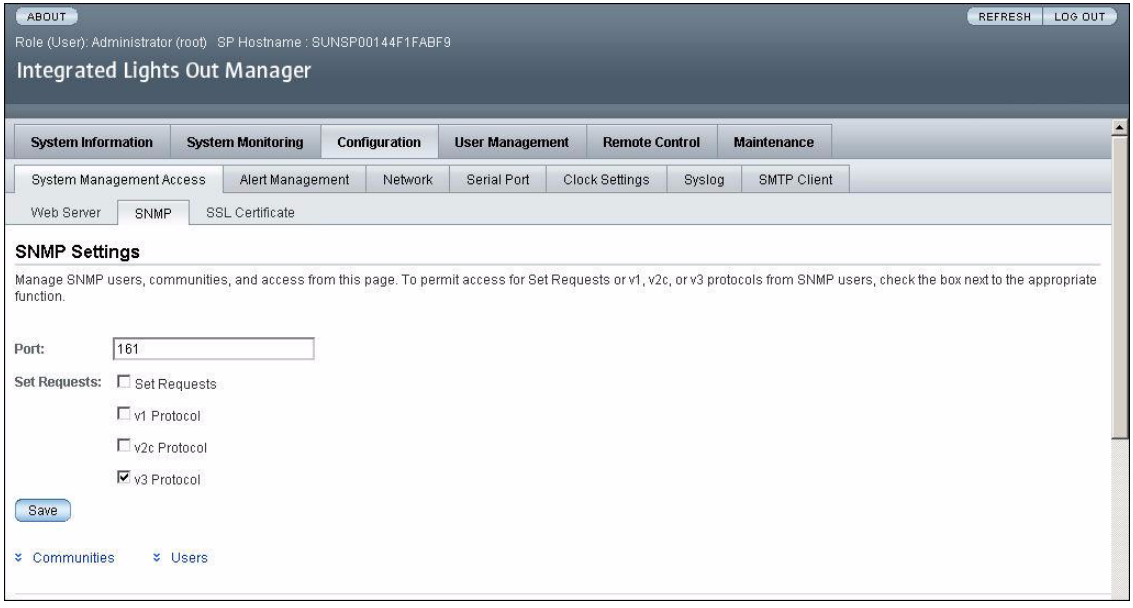
1. **Melden Sie sich bei ILOM als Administrator an, um die Webbenutzeroberfläche zu öffnen.**

   SNMP-Einstellungen können nur geändert werden, wenn Sie bei ILOM mit Administratorberechtigungen angemeldet sind.

2. **Wählen Sie Configuration --> System Management Access --> SNMP.**

   Die Seite SNMP Settings wird angezeigt.

**ABBILDUNG 10-1** Seite SNMP Settings



3. **Geben Sie die Anschlussnummer in das Textfeld Port ein.**

4. **Aktivieren oder deaktivieren Sie das Kontrollkästchen Set Requests, um die Option Set Requests zu aktivieren bzw. zu deaktivieren.**

   Wenn Set Requests deaktiviert ist, sind alle SNMP-Objekte schreibgeschützt.

5. **Aktivieren Sie ein Kontrollkästchen, um SNMP v1, v2c oder v3 zu aktivieren.**

   SNMP v3 ist standardmäßig aktiviert. Sie können die Protokollversionen v1, v2c und v3 aktivieren bzw. deaktivieren.

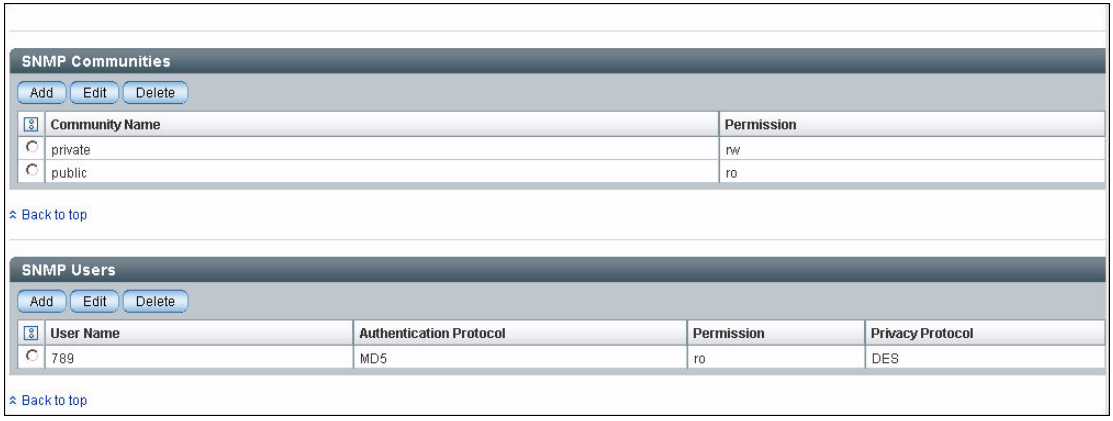
6. **Klicken Sie auf Save.**

---

**Hinweis –** Unten auf der Seite können Sie außerdem, wie in ABBILDUNG 10-2 dargestellt, SNMP-Communitys oder -Benutzer hinzufügen, bearbeiten und löschen.

---

**ABBILDUNG 10-2** SNMP-Communitys und -Benutzer




## ▼ Hinzufügen oder Bearbeiten eines SNMP-Benutzerkontos mithilfe der Webbenutzeroberfläche

Führen Sie diese Schritte durch, um ein SNMP v3-Benutzerkonto hinzuzufügen oder zu bearbeiten:

1. **Melden Sie sich bei ILOM als Administrator an, um die Webbenutzeroberfläche zu öffnen.**

   Ein SNMP-Benutzer bzw. -Benutzerkonto kann nur hinzugefügt werden, wenn Sie bei ILOM mit Administratorberechtigungen angemeldet sind.

2. **Wählen Sie Configuration --> System Management Access --> SNMP.**

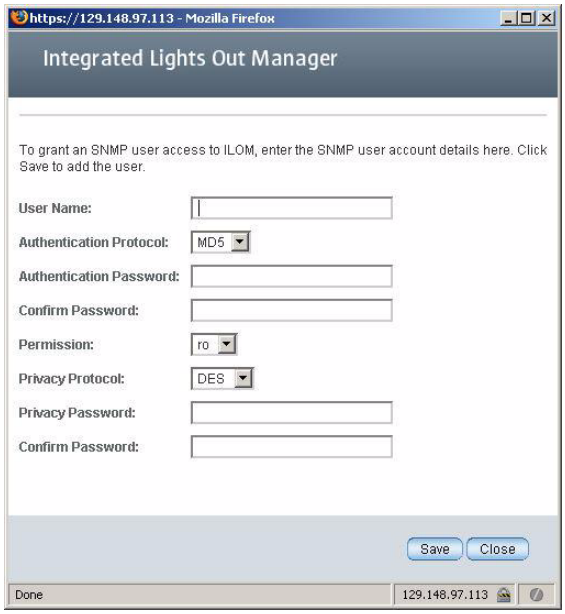
   Die Seite SNMP Settings wird angezeigt.

3. **Klicken Sie auf die Verknüpfung Users, oder führen Sie einen Bildlauf zur Liste SNMP Users durch.**

4. **Klicken Sie unterhalb der Liste SNMP Users auf Add oder Edit.**

   Das Dialogfeld Add oder Edit wird, wie in ABBILDUNG 10-3 **dargestellt, angezeigt.**

**ABBILDUNG 10-3** Dialogfeld Add SNMP User




5. **Geben Sie einen Benutzernamen in das Textfeld User Name ein.**

   Der Benutzername darf maximal 35 Zeichen lang sein. Er muss mit einem Buchstaben beginnen und darf keine Leerzeichen enthalten.

6. **Wählen Sie im Dropdown-Listenfeld Authentication Protocol entweder Message Digest 5 (MD5) oder Secure Hash Algorithm (SHA).**

7. **Geben Sie ein Passwort in das Textfeld Authentication Password ein.**

   Das Authentifizierungspasswort muss zwischen 8 und 16 Zeichen lang sein und darf keine Doppelpunkte oder Leerzeichen enthalten. Das Passwort unterscheidet zwischen Groß- und Kleinschreibung.

8. **Geben Sie das Authentifizierungspasswort erneut in das Textfeld Confirm Password ein.**

9. **Wählen Sie im Dropdown-Listenfeld Permissions den Eintrag ro (schreibgeschützt) oder rw (Lesen/Schreiben).**

10. **Wählen Sie im Dropdown-Listenfeld Privacy Protocol den Eintrag DES oder None.**
11. **Geben Sie ein Passwort in das Textfeld Privacy Password ein.**

    Das Datenschutzpasswort muss zwischen 8 und 16 Zeichen lang sein und darf keine Doppelpunkte oder Leerzeichen enthalten. Das Passwort unterscheidet zwischen Groß- und Kleinschreibung.
12. **Geben Sie das Passwort erneut in das Textfeld Confirm Password ein.**
13. **Klicken Sie auf Save.**

## ▼ Löschen eines SNMP-Benutzerkontos mithilfe der Webbenutzeroberfläche

Führen Sie diese Schritte durch, um ein SNMP v3-Benutzerkonto zu löschen:

1. **Melden Sie sich bei ILOM als Administrator an, um die Webbenutzeroberfläche zu öffnen.**

   SNMP-Einstellungen können nur geändert werden, wenn Sie bei Konten mit Administratorberechtigungen angemeldet sind.
2. **Wählen Sie Configuration --> System Management Access --> SNMP.**

   Die Seite SNMP Settings wird angezeigt.
3. **Klicken Sie auf die Verknüpfung Users, oder führen Sie einen Bildlauf zur Liste SNMP Users durch.**
4. **Aktivieren Sie das Optionsfeld des zu löschenden SNMP-Benutzerkontos.**
5. **Klicken Sie unterhalb der Liste SNMP Users auf Delete.**

   Ein Bestätigungsdialogfeld wird angezeigt.
6. **Klicken Sie auf OK, um das Benutzerkonto zu löschen.**

## ▼ Hinzufügen oder Bearbeiten einer SNMP-Community mithilfe der Webbenutzeroberfläche

Führen Sie diese Schritte durch, um eine SNMP v1- oder v2-Community hinzuzufügen oder zu bearbeiten:

1. **Melden Sie sich bei ILOM als Administrator an, um die Webbenutzeroberfläche zu öffnen.**

   SNMP-Communitys können nur hinzugefügt oder bearbeitet werden, wenn Sie bei Konten mit Administratorberechtigungen angemeldet sind.

2. **Wählen Sie Configuration --> System Management Access --> SNMP.**

   Die Seite SNMP Settings wird angezeigt.

3. **Klicken Sie auf die Verknüpfung Communities, oder führen Sie einen Bildlauf zur Liste Communities durch.**

4. **Klicken Sie für die Liste SNMP Communities auf Add oder Edit.**

   Das Dialogfeld Add oder Edit wird angezeigt.

5. **Geben Sie den Namen der Community in das Feld Community Name ein.**

   Der Community-Name darf maximal 35 Zeichen lang sein. Er muss mit einem Buchstaben beginnen und darf keine Leerzeichen enthalten.

6. **Wählen Sie im Dropdown-Listenfeld Permissions den Eintrag ro (schreibgeschützt) oder rw (Lesen/Schreiben).**

7. **Klicken Sie auf Save.**

## ▼ Löschen einer SNMP-Community mithilfe der Webbenutzeroberfläche

Führen Sie diese Schritte durch, um eine SNMP v1- oder v2-Community zu löschen:

1. **Melden Sie sich bei ILOM als Administrator an, um die Webbenutzeroberfläche zu öffnen.**

   Eine SNMP-Comunity kann nur gelöscht werden, wenn Sie bei Konten mit Administratorberechtigungen angemeldet sind.

2. **Wählen Sie Configuration --> System Management Access --> SNMP.**

   Die Seite SNMP Settings wird angezeigt.

3. **Klicken Sie auf die Verknüpfung Communities, oder führen Sie einen Bildlauf zur Liste Communities durch.**

4. **Aktivieren Sie das Optionsfeld der zu löschenden SNMP-Community.**

5. **Klicken Sie auf Delete.**

   Ein Bestätigungsdialogfeld wird angezeigt.

6. **Klicken Sie auf OK, um die SNMP-Community zu löschen.**

## ▼ Konfigurieren von SNMP-Trap-Zielen mithilfe der Webbenutzeroberfläche

Führen Sie diese Schritte durch, um die Ziele zu konfigurieren, an die die SNMP-Traps gesendet werden.

1. **Melden Sie sich bei ILOM als Administrator an, um die Webbenutzeroberfläche zu öffnen.**

   SNMP-Trap-Ziele können nur konfiguriert werden, wenn Sie bei Konten mit Administratorberechtigungen angemeldet sind.

2. **Wählen Sie Configuration --> Alert Management.**

   Die Seite Alert Settings wird angezeigt. Auf dieser Seite befindet sich die Tabelle mit den konfigurierten Alarmen.

3. **Wählen Sie im Dropdown-Listenfeld Actions den Eintrag Edit.**

   Das Dialogfeld Create oder Modify wird angezeigt.

4. **Wählen Sie in dem Dialogfeld im Dropdown-Listenfeld die Stufe des Alarms aus.**

5. **Wählen Sie im Dropdown-Listenfeld Type den Eintrag SNMP Trap.**

6. **Geben Sie die IP-Adresse des SNMP-Trap-Ziels an, die SNMP-Version und den Community- oder Benutzernamen.**

7. **Klicken Sie auf Save, um die Änderungen zu übernehmen.**

# SNMP-Beispiele

In diesem Abschnitt finden Sie verschiedene Beispiele für die Verwendung von `net-snmp` zum Abfragen des SNMP-Agent auf einem ILOM-SP.

Laden Sie als Erstes die neueste Version (Version 5.2.1 oder höher) von `net-snmp`, die mit dem Betriebssystem Ihrer Verwaltungsstation zusammenarbeitet, herunter, und installieren Sie sie:

```
http://net-snmp.sourceforge.net/
```

`net-snmp` installiert alle Standard-MIBs (SNMPv2-MIB, SNMP-FRAMEWORK-MIB und ENTITY-MIB), die von ILOM unterstützt werden. Sie müssen die Dateien SUN-PLATFORM-MIB.mib, SUN-ILOM-CONTROL-MIB.mib, SUN-HW-TRAP-MIB.mib und SUN-ILOM-PET-MIB.mib herunterladen und in dem Verzeichnis speichern, aus dem Tools von `net-snmp` MIBs laden. Zusätzliche Informationen finden Sie unter folgender URL:

```
http://net-snmp.sourceforge.net/wiki/index.php/
TUT:Using_and_loading_MIBS
```

## ▼ Anzeigen und Konfigurieren von SNMP-Einstellungen

Konfigurieren Sie den SP oder das CMM wie in den vorherigen Abschnitten beschrieben, und führen Sie dann diese Schritte aus, um SNMP-Einstellungen anzuzeigen und zu konfigurieren:

1. **Wechseln Sie in das Verzeichnis** `/SP/services/snmp`**, indem Sie Folgendes eingeben:**

   -> **`cd /SP/services/snmp`**

2. **Geben Sie in diesem Verzeichnis den Befehl** `show` **ein, um SNMP-Einstellungen anzuzeigen.**

```
-> show
   /SP/services/snmp
   Targets:
     communities
     users
   Properties:
     engineid = none
     port = 161
     sets = disabled
     v1 = disabled
     v2c = disabled
     v3 = enabled
  Commands:
     cd
     set
     show
```

3. **Konfigurieren Sie SNMP-Einstellungen.**

   Beispiel:

   - Legen Sie `v2c` auf `enabled` fest, indem Sie Folgendes eingeben:

     -> **`set v2c=enabled`**

   - Legen Sie `sets` auf `enabled` fest, indem Sie Folgendes eingeben:

     -> **`set sets=enabled`**

4. **Zeigen Sie die Communitys an, indem Sie Folgendes eingeben:**

   -> **show communities**

```
-> show communities
/SP/services/snmp/communities
Targets:
  public
Properties:
Commands:
  cd
  create
  delete
  show
```

5. **Zeigen Sie die öffentlichen Communitys an, indem Sie Folgendes eingeben:**

   -> **show communities/public**

```
-> show communities/public
/SP/services/snmp/communities/public
Targets:
Properties:
  permission = ro
Commands:
  cd
  set
  show
```

6. **Erstellen Sie private Communitys mit Schreib-/Lesezugriff, indem Sie Folgendes eingeben:**

   -> **create communities/private permission=rw**

## ▼ Abrufen von Informationen mithilfe der Befehl `snmpget` oder `snmpwalk net-snmp`

1. **Geben Sie den Befehl** `snmpget` **ein, um bestimmte Informationen abzurufen.**

   Beispiel:

```
$ snmpget -v 2c -c public -m ALL <sp_ip> sysObjectID.0 sysUpTime.0 sysLocation.0
        SNMPv2-MIB::sysObjectID.0 =
        OID:SUN-FIRE-SMI-MIB::sunBladeX8400ServerModule
        SNMPv2-MIB::sysUpTime.0 = Timeticks: (17523) 0:02:55.23
        SNMPv2-MIB::sysLocation.0 = STRING:
```

2. **Geben Sie den Befehl** `snmpwalk` **ein, um Informationen über diskrete Komponenten abzurufen.**

   Beispiel:

```
$ snmpwalk -v 2c -c public -m ALL <sp_ip> entPhysicalName
        ENTITY-MIB::entPhysicalName.1 = STRING: /SYS
        ENTITY-MIB::entPhysicalName.2 = STRING: /SYS/OK2RM
        ENTITY-MIB::entPhysicalName.3 = STRING: /SYS/SERVICE
        ENTITY-MIB::entPhysicalName.4 = STRING: /SYS/OK
        ENTITY-MIB::entPhysicalName.5 = STRING: /SYS/LOCATE
        ENTITY-MIB::entPhysicalName.6 = STRING: /SYS/LOCATE_BTN
        ENTITY-MIB::entPhysicalName.7 = STRING: /SYS/POWER_BTN
        ENTITY-MIB::entPhysicalName.8 = STRING: /SYS/T_AMB
        ENTITY-MIB::entPhysicalName.9 = STRING: /SYS/P0
```

## ▼ Festlegen von Informationen mithilfe von `snmpset`

- **Geben Sie den Befehl** `snmpset` **ein, um die Position von Geräten zu ändern.**

  Beispiel:

```
$ snmpset -v 2c -c private -m ALL <sp_ip> sysLocation.0 s "<Position>"
```

  Beispiel:

```
SNMPv2-MIB::sysLocation.0 = STRING: ILOM Dev Lab
```

## ▼ Empfangen von Traps mithilfe von `snmptrapd`

- **Geben Sie den Befehl** `snmptrapd` **ein, um Trap-Informationen zu empfangen.**

  Beispiel:

```
$ /usr/sbin/snmptrapd -m ALL -f -Lo
SNMP-Trap-Beispiel:
        2007-05-21 08:46:41 ban3c9sp4 [10.8.136.94]:
        SNMPv2-MIB::sysUpTime.0 = Timeticks: (1418) 0:00:14.18
        SNMPv2-MIB::snmpTrapOID.0 = OID:
        SUN-HW-TRAP-MIB::sunHwTrapPowerSupplyError
        SUN-HW-TRAP-MIB::sunHwTrapSystemIdentifier.0 = STRING:
        SUN-HW-TRAP-MIB::sunHwTrapChassisId.0 = STRING:
        ban6c4::0000000000 SUN-HW-TRAP-MIB::sunHwTrapProductName.0
        = STRING:   SUN-HW-TRAP-MIB::sunHwTrapComponentName.0 =
        STRING: /PS3/FAN_ERR
        SUN-HW-TRAP-MIB::sunHwTrapAdditionalInfo.0 = STRING: Predictive
        Failure Asserted    SUN-HW-TRAP-MIB::sunHwTrapAssocObjectId.0 =
        OID: SNMPv2-SMI::zeroDotZero
```

KAPITEL 11

# Aktualisieren der ILOM-Firmware

Durch den Aktualisierungsprozess der ILOM-Firmware können Sie neue ILOM-Firmware installieren und andere Module Ihrer Plattform aktualisieren, wie z. B. das BIOS auf x64-Plattformen, den OpenBoot PROM und die Hypervisor-Software auf SPARC-Plattformen.

Dieses Kapitel enthält folgende Abschnitte:


- „Prozess der Firmwareaktualisierung“ auf Seite 203
- „ILOM-Firmwareaktualisierung – Überblick“ auf Seite 204
  - „Anzeigen von ILOM-Versionsinformationen mithilfe der CLI“ auf Seite 204
  - „Aktualisieren der ILOM-Firmware mithilfe der CLI“ auf Seite 205
  - „Anzeigen von ILOM-Versionsinformationen mithilfe der Webbenutzeroberfläche“ auf Seite 205
  - „Aktualisieren der ILOM-Firmware mithilfe der Webbenutzeroberfläche“ auf Seite 206
  - „Zurücksetzen des ILOM-SP“ auf Seite 207


## Prozess der Firmwareaktualisierung

Lesen Sie diese Vorsichtsmaßnahme und die Richtlinien, bevor Sie die Firmware aktualisieren:

**Achtung –** Fahren Sie das Hostbetriebssystem herunter, bevor Sie den Vorgang fortsetzen. ILOM versucht, das Betriebssystem ordnungsgemäß herunterzufahren. Sollte ein ordnungsgemäßes Herunterfahren nicht möglich sein, erzwingt ILOM das Herunterfahren, wodurch es zu Fehlern im Dateisystem kommen kann.

- Der Aktualisierungsprozess der Firmware nimmt ungefähr fünf Minuten in Anspruch. Während dieses Zeitraums dürfen keine anderen Aufgaben in ILOM ausgeführt werden.
- Netzwerkfehler während des Hochladens der Firmwaredatei führen zu einer Zeitüberschreitung. Dies wiederum veranlasst ILOM zu einem Neustart mit der *aktuell* installierten Version der ILOM-Firmware.

## ILOM-Firmwareaktualisierung – Überblick

1. Laden Sie das neue Firmwareabbild herunter.
2. Kopieren Sie das Abbild für eine Aktualisierung über die CLI auf einen TFTP-Server bzw. für eine Aktualisierung über die Webbenutzeroberfläche in ein lokales Dateisystem.
3. Melden Sie sich als Benutzer mit Administratorberechtigungen an.
4. Aktualisieren Sie die Firmware auf jedem Service-Prozessor (SP) und/oder CMM (Chassis Monitoring Module) im System mithilfe der CLI oder der Webbenutzeroberfläche.
5. Nach Abschluss der Firmwareaktualisierung führt das System *automatisch* einen Neustart aus.

## ▼ Anzeigen von ILOM-Versionsinformationen mithilfe der CLI

1. **Melden Sie sich bei der SSH als Benutzer mit Administratorberechtigungen an.**
2. **Geben Sie an der Befehlseingabeaufforderung** `version` **ein.**

   Folgende Informationen werden angezeigt:

```
SP firmware #.#.#.#
SP firmware build number: #####
SP firmware date: Fri Apr 27 14:03:21 EDT 2007
SP filesystem version: #.#.##
```

## ▼ Aktualisieren der ILOM-Firmware mithilfe der CLI

1. **Melden Sie sich als Benutzer mit Administratorberechtigungen an.**
2. **Geben Sie folgenden Befehl ein, um das neue ILOM-Firmwareabbild herunterzuladen:**

   **->load -source** *tftpURL*

   Beispiel:

```
-> load -source tftp://xxx.xxx.xxx.xxx/Dateiname.pkg

NOTE: A firmware upgrade will cause the server and ILOM to
      be reset. It is recommended that a clean shutdown of
      the server be done prior to the upgrade procedure.
      An upgrade takes about 6 minutes to complete. ILOM
      will enter a special mode to load new firmware. No
      other tasks can be performed in ILOM until the
      firmware upgrade is complete and ILOM is reset.

Are you sure you want to load the specified file (y/n)? y
Do you want to preserve the configuration (y/n)? y
. . . . . .
Preserving configuration. Please wait.
Done preserving configuration.


Firmware update is complete.
ILOM will now be restarted with the new firmware.
```

## ▼ Anzeigen von ILOM-Versionsinformationen mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich als Benutzer mit Administratorberechtigungen an.**
2. **Wählen Sie User Management -->Version.**

Die aktuellen Firmwareversionsinformationen werden angezeigt.

## ▼ Aktualisieren der ILOM-Firmware mithilfe der Webbenutzeroberfläche

1. **Melden Sie sich als Benutzer mit Administratorberechtigungen an.**
2. **Wählen Sie Maintenance --> Firmware Upgrade.**

   Die Seite Firmware Upgrade wird angezeigt.
3. **Klicken Sie auf Enter Upgrade Mode.**

   In dem daraufhin angezeigten Dialogfeld werden Sie zur Bestätigung aufgefordert, dass in den Aktualisierungsmodus gewechselt werden soll.
4. **Klicken Sie auf OK, um in den Aktualisierungsmodus zu wechseln, oder auf Cancel, um den Prozess zu beenden.**

   ILOM beendet den normalen Betrieb und bereitet sich auf eine Flash-Aktualisierung vor.
5. **Geben Sie den Pfad zu der neuen ILOM-Flash-Abbilddatei in das Feld Select Image File to Upload ein, oder klicken Sie auf Browse, um die Firmwareaktualisierungsdatei zu suchen und auszuwählen.**

   Dateien mit den Erweiterungen `.pkg` und `.ima` können verwendet werden, bevorzugt wird jedoch die Erweiterung `.pkg`.

**ABBILDUNG 11-1** Seite Firmware Upgrade

ABOUT
REFRESH
LOG OUT
Role (User): Administrator (root) SP Hostname : SUNSP00144F1FABF9
Integrated Lights Out Manager
System Information
System Monitoring
Configuration
User Management
Remote Control
Maintenance
Firmware Upgrade
Reset SP
Firmware Upgrade
A firmware upgrade will cause ILOM to be reset and may also reset the server if the BIOS gets updated. It is recommended that a clean shutdown of the server be done prior to the upgrade procedure. An upgrade takes about 6 minutes to complete. ILOM will enter a special mode to load new firmware. Users signed in through other sessions will lose connectivity when ILOM is reset.
Enter Upgrade Mode

6. **Klicken Sie auf Upload, oder klicken Sie auf Cancel, um den Prozess zu beenden.**

   Die gewählte Datei wird hochgeladen und überprüft, dass es sich um das richtige Aktualisierungsabbild für Ihren SP oder das CMM handelt.

   Dieser Prozess dauert bei einer schnellen Netzwerkverbindung ungefähr eine Minute.

7. **Wenn die Seite Verify Firmware Image angezeigt wird, klicken Sie auf OK.**

8. **Aktivieren Sie Preserve Configuration, um Ihre bisherigen ILOM-Einstellungen beizubehalten. Ohne die Aktivierung dieser Option werden die Einstellungen mit den Firmwarestandardeinstellungen überschrieben.**

9. **Klicken Sie auf Start Upgrade, oder klicken Sie auf Cancel, um den Prozess zu beenden.**

   Wenn Sie auf Start Upgrade klicken, wird in einem Fortschrittsbildschirm angezeigt, dass das Firmwareabbild aktualisiert wird. Sobald der Aktualisierungsstatus 100 % erreicht hat, ist die Firmwareaktualisierung abgeschlossen.

   Nach Abschluss der Aktualisierung führt das System *automatisch* einen Neustart aus.

10. **Nachdem der Neustart des SP und/oder CMM fertig gestellt ist, stellen Sie mithilfe des Browsers eine neue Verbindung mit ILOM her.**

## ▼ Zurücksetzen des ILOM-SP

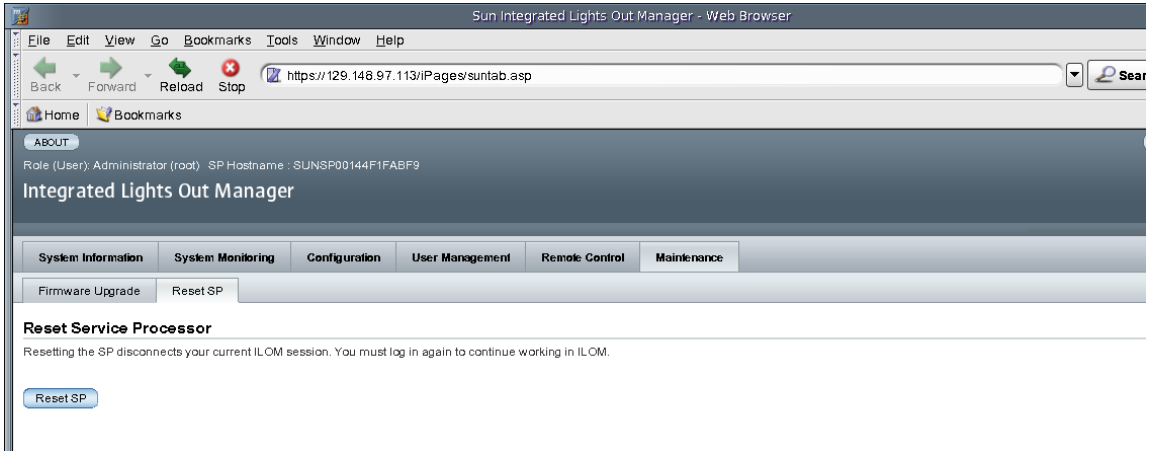
Wenn der ILOM-Service-Prozessor (SP) zurückgesetzt werden muss, kann dies ohne Auswirkungen auf das Hostbetriebssystem erfolgen. Durch das Zurücksetzen eines SP wird jedoch Ihre aktuelle ILOM-Sitzung unterbrochen, und der SP kann während des Zurücksetzens nicht verwaltet werden.

1. **Melden Sie sich als Benutzer mit Administratorberechtigungen an.**

2. **Wählen Sie Maintenance --> Reset SP.**

   Die Seite Reset Service Processor wird angezeigt.

**ABBILDUNG 11-2** Seite Reset Service Processor



3. **Klicken Sie auf die Schaltfläche Reset SP, um den ILOM-SP (Service-Prozessor) zurückzusetzen.**

   ILOM führt einen Neustart aus. Während dieses Vorgangs kann nicht auf die Webbenutzeroberfläche zugegriffen werden.

KAPITEL 12

# Entfernte Verwaltung von x64-Servern mithilfe der ILOM-Remotekonsole

Die ILOM-Remotekonsole wird auf allen Servern mit x64-Prozessoren unterstützt. Die ILOM-Remotekonsole wird zurzeit auf SPARC-Servern nicht unterstützt.

Dieses Kapitel enthält folgende Abschnitte:


- „ILOM-Remotekonsole – Überblick“ auf Seite 210
  - „Einzel- und Mehrfachverwaltungsansichten für entfernte Hostserver“ auf Seite 211
  - „Voraussetzungen für die Installation“ auf Seite 213
  - „Anschlüsse und Protokolle für die Netzwerkkommunikation“ auf Seite 213
  - „Benutzerkonto mit Administrator-Rolle – Anmeldeauthentifizierung erforderlich“ auf Seite 213
- „Starten und Konfigurieren von ILOM für die entfernte Verwaltung“ auf Seite 214
  - „Herstellen einer Verbindung mit der ILOM-Webbenutzeroberfläche“ auf Seite 215
  - „Konfigurieren von ILOM-Einstellungen für entfernte Steuerung mithilfe der Webbenutzeroberfläche“ auf Seite 216
- „Starten und Konfigurieren der ILOM-Remotekonsole für die entfernte Verwaltung von x64-Servern“ auf Seite 220
  - „Starten der ILOM-Remotekonsole mithilfe der ILOM-Webbenutzeroberfläche“ auf Seite 220
  - „Hinzufügen einer neuen Serversitzung“ auf Seite 222
  - „Starten, Beenden und Neustarten der Geräteumleitung“ auf Seite 222
  - „Umleiten von Tastatur- und Mausgeräten“ auf Seite 223
  - „Steuern von Tastaturmodi und Sendeoptionen für Tasten“ auf Seite 224
  - „Umleiten von Speichergeräten“ auf Seite 225
  - „Beenden der ILOM-Remotekonsole“ auf Seite 226
- „Betriebsszenarien für die CD- und Diskettenumleitung“ auf Seite 227

# ILOM-Remotekonsole – Überblick

Die ILOM-Remotekonsole ist eine Java-Anwendung, die über die ILOM-Webbenutzeroberfläche gestartet werden kann. Bei Verwendung der ILOM-Remotekonsole können Sie die folgenden Geräte auf einem entfernten x64-Hostserver entfernt umleiten und steuern:

- Tastatur
- Maus
- Bildschirmkonsolenanzeige
- Speichergeräte oder Abbilder (CD/DVD, Diskette)

Mit der ILOM-Remotekonsole können sich die Geräte an Ihrem lokalen Client so verhalten, als ob sie direkt an einen entfernten Hostserver angeschlossen wären. So können Sie beispielsweise mit der Umleitungsfunktion bei Verwendung einer Netzwerkverbindung mit dem entfernten Hostserver folgende Aktionen ausführen:

- Installieren von Software auf einem entfernten Hostserver von einem lokalen Medienlaufwerk aus.
- Ausführen von Befehlszeilendienstprogrammen auf einem entfernten Hostserver von einem lokalen Client aus.
- Zugreifen auf und Ausführen von Programmen mit grafischen Benutzeroberflächen auf einem entfernten Hostserver von einem lokalen Client aus.
- Entferntes Konfigurieren von Leistungsmerkmalen von Servern mit x64-Prozessoren von einem lokalen Client aus.
- Entferntes Verwalten von Richtlinien von Servern mit x64-Prozessoren von einem lokalen Client aus.
- Entferntes Überwachen von Elementen von Servern mit x64-Prozessoren von einem lokalen Client aus.
- Ausführen beinahe aller Aufgaben für auf x64-Prozessoren basierende Software von einem lokalen Client aus, die Sie normalerweise auch ausführen könnten, wenn Sie sich an einem entfernten Hostserver befänden.

# Einzel- und Mehrfachverwaltungsansichten für entfernte Hostserver

Die ILOM-Remotekonsole unterstützt sowohl Einzel- als auch Mehrfachverwaltungsansichten für entfernte Hostserver. Einzel- und Mehrfachverwaltungsansichten für Server werden zurzeit auf allen Servern mit x64-Prozessoren unterstützt.

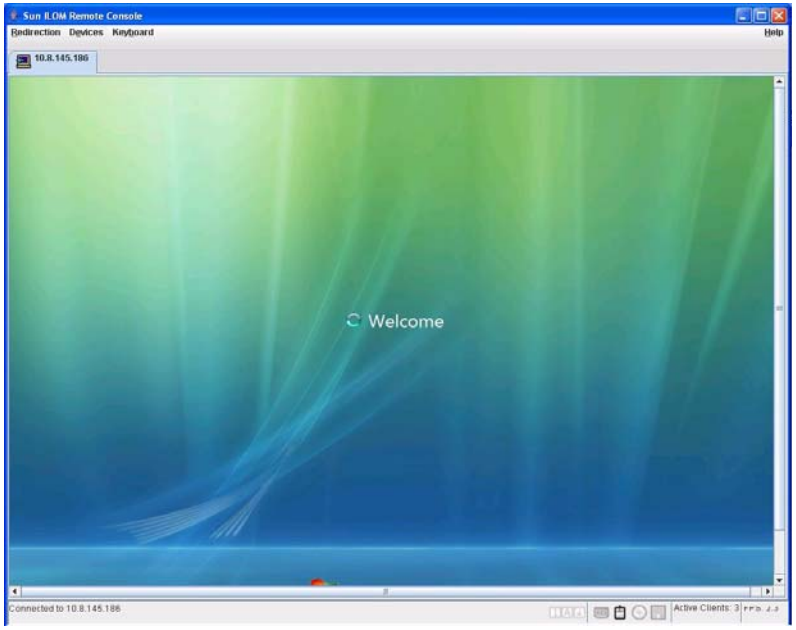
- **Einzelverwaltungsansicht für entfernte x64-Server** – Sie können die ILOM-Remotekonsole für die Verwaltung eines einzelnen entfernten Hostservers in einem einzelnen Fenster starten und die entfernten Tastatur-, Bildschirmanzeige-, Maus- und Speicherleistungsmerkmale (Keyboard, Video, Mouse, Storage, KVMS) nutzen.

---

**Hinweis –** Einzelverwaltungsansichten für entfernte Server werden beim Herstellen einer Verbindung mit der IP-Adresse eines beliebigen x64-Server-SP (Service-Prozessor) unterstützt. Weitere Informationen zu diesem Thema finden Sie unter „Starten und Konfigurieren der ILOM-Remotekonsole für die entfernte Verwaltung von x64-Servern“ auf Seite 220.

---

**ABBILDUNG 12-1** Einzelverwaltungsansicht für einen Server



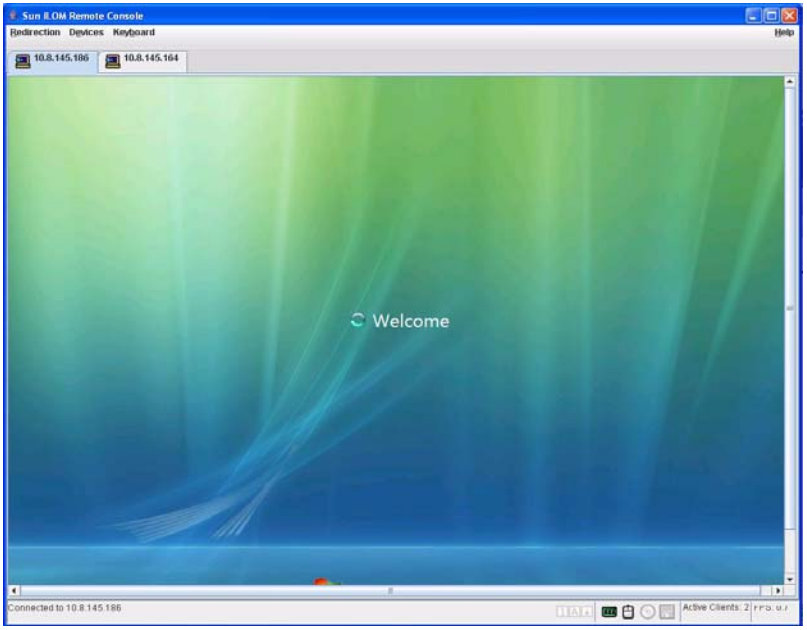
- **Mehrfachverwaltungsansichten für entfernte x64-Server** – Sie können die ILOM-Remotekonsole für die Verwaltung mehrerer entfernter x64-Server in einem einzelnen Fenster starten und die entfernten Tastatur-, Bildschirmanzeige-, Maus- und Speicherleistungsmerkmale (Keyboard, Video, Mouse, Storage, KVMS) nutzen.

---

**Hinweis –** Mehrfachverwaltungsansichten für entfernte Server werden unter folgenden Umständen unterstützt: Wenn Sie (1) eine Verbindung mit der IP-Adresse eines beliebigen x64-Blade-Server-CMM (Chassis Monitoring Module) herstellen, oder wenn Sie (2) eine neue ILOM-Remotekonsolensitzung hinzufügen, um einen weiteren entfernten x64-Server zu verwalten. Weitere Informationen zu diesem Thema finden Sie unter „Starten und Konfigurieren der ILOM-Remotekonsole für die entfernte Verwaltung von x64-Servern“ auf Seite 220.

---

**ABBILDUNG 12-2** Mehrfachverwaltungsansichten für Server



# Voraussetzungen für die Installation

Für die ILOM-Remotekonsole muss keine zusätzliche Hardware oder Software installiert werden. Sie ist in die ILOM-Software integriert. Zum Ausführen der ILOM-Remotekonsole muss jedoch die folgende Software auf dem lokalen Client installiert sein:

- **Webbrowser** – Folgende Browser werden unterstützt: Internet Explorer 6.0 oder höher, Mozilla 1.7.5 oder höher, Mozilla Fire Fox 1.0 oder höher.
- **JRE 1.5 oder höher (Java 5.0 oder höher)** – Informationen zum Herunterladen der Java 1.5-Laufzeitumgebung finden Sie unter `http://java.com`.

# Anschlüsse und Protokolle für die Netzwerkkommunikation

Die ILOM-Remotekonsole kommuniziert mit einem entfernten Hostserver-SP mithilfe der folgenden Netzwerkprotokolle und -anschlüsse.

**TABELLE 12-1** Netzwerkanschlüsse und -protokolle der SP ILOM-Remotekonsole

| Anschluss | Protokoll | SP - ILOM-Remotekonsole |
|---|---|---|
| 5120 | TCP | CD |
| 5123 | TCP | Diskette |
| 5121 | TCP | Tastatur und Maus |
| 7578 | TCP | Bildschirmanzeige |

**Hinweis –** Bei der entfernten Verwaltung von Servern mithilfe von CMM ILOM müssen Sie den Zugriff auf alle SP-Remotekonsolenanschlüsse (5120, 5121, 5123 und 7578) konfigurieren.

# Benutzerkonto mit Administrator-Rolle - Anmeldeauthentifizierung erforderlich

Zum Starten der ILOM-Remotekonsole über die ILOM-Webbenutzeroberfläche müssen Sie sich zuerst mit einem Administrator-Rollenkonto bei ILOM anmelden (Benutzername und Passwort mit Administrator-Rolle).

- Wenn Sie sich bei ILOM mit einem *Operator-Rollenkonto* angemeldet und versucht haben, die ILOM-Remotekonsole zu starten, werden Sie von ILOM aufgefordert, sich mit einem gültigen Administrator-Rollenkonto über das Dialogfeld Login anzumelden.
- Wenn Sie sich anfänglich bei ILOM mit einem *Administrator-Rollenkonto* angemeldet und die ILOM-Remotekonsole gestartet haben, wird automatisch die Umleitungsseite der ILOM-Remotekonsole angezeigt. Sie werden aber in jedem Fall jedes Mal von der ILOM-Remotekonsole zum Anmelden aufgefordert, wenn Sie die Umleitung beenden und wieder starten oder erneut starten.

---

**Hinweis –** Wenn die Funktion Single Sign On (Einmalanmeldung) in ILOM deaktiviert ist, werden Benutzer mit Administrator-Rollenberechtigungen erneut zum Anmelden bei ILOM über das Dialogfeld Login aufgefordert. Zusätzliche Informationen zur Single Sign On-Funktion finden Sie unter „Single Sign On“ auf Seite 69.

---

# Starten und Konfigurieren von ILOM für die entfernte Verwaltung

Vor dem Starten der ILOM-Remotekonsole müssen Sie die ILOM-Webbenutzeroberfläche starten und ILOM für die entfernte Verwaltung konfigurieren.

- **Herstellen einer Verbindung mit der ILOM-Webbenutzeroberfläche** – Sie müssen eine Verbindung mit der ILOM-Webbenutzeroberfläche des Servers (SP oder CMM), der entfernt verwaltet werden soll, herstellen. Diesbezügliche Anweisungen erhalten Sie unter „Herstellen einer Verbindung mit der ILOM-Webbenutzeroberfläche“ auf Seite 215.
- **Konfigurieren der ILOM-Einstellungen für entfernte Steuerung** – Vor dem entfernten Verwalten eines x64-Servers mithilfe der ILOM-Remotekonsole müssen Sie zuerst die ILOM-Einstellungen für die entfernte Verwaltung konfigurieren: *Konsolenumleitung*, *unterstützter Mausmodus*, *Stromversorgungszustände des entfernten Hosts* sowie *Diagnosetests beim Starten des Computers*. Weitere Informationen zu diesem Thema finden Sie unter „Konfigurieren von ILOM-Einstellungen für entfernte Steuerung mithilfe der Webbenutzeroberfläche“ auf Seite 216.

---

**Hinweis –** Normalerweise richten Sie die Steuerungseinstellungen für die entfernte Verwaltung, mit Ausnahme der Stromversorgungszustände des entfernten Hosts, einmalig in ILOM ein.

---

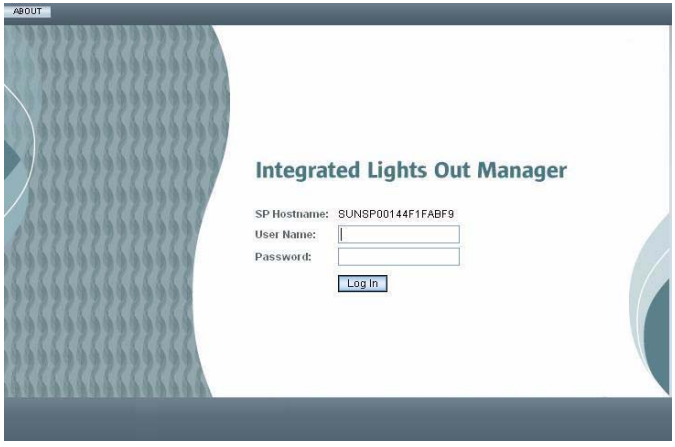
## ▼ Herstellen einer Verbindung mit der ILOM-Webbenutzeroberfläche

Führen Sie diese Schritte durch, um eine Verbindung mit der ILOM-Webbenutzeroberfläche herzustellen:

1. **Öffnen Sie einen Webbrowser, geben Sie die IP-Adresse eines entfernt zu verwaltenden x64-Server-SP oder x64-CMM an, und drücken Sie die Eingabetaste.**

   Die Seite ILOM Login wird angezeigt.

**ABBILDUNG 12-3** Seite ILOM Login




2. **Geben Sie auf der Seite ILOM Login den Benutzernamen mit Passwort eines gültigen Administrator-Rollenkontos ein, und drücken Sie die Eingabetaste.**

---

**Tipp –** Das vorkonfigurierte Administrator-Rollenkonto, das in ILOM enthalten ist lautet `root/ changeme`. Zusätzliche Informationen zu diesem vorkonfigurieren Konto finden Sie unter „Vorkonfigurierte ILOM-Administratorkonten“ auf Seite 66.

---

## ▼ Konfigurieren von ILOM-Einstellungen für entfernte Steuerung mithilfe der Webbenutzeroberfläche

### Voraussetzung:

- Bestehende Verbindung mit der ILOM-Webbenutzeroberfläche des entfernten Hostservers (SP oder CMM). Diesbezügliche Anweisungen erhalten Sie unter „Herstellen einer Verbindung mit der ILOM-Webbenutzeroberfläche“ auf Seite 215.

Führen Sie diese Schritte durch, um ILOM-Einstellungen für die entfernte Verwaltung zu konfigurieren:

1. **Klicken Sie in der CMM- oder SP-ILOM-Webbenutzeroberfläche auf die Registerkarte Remote Control.**

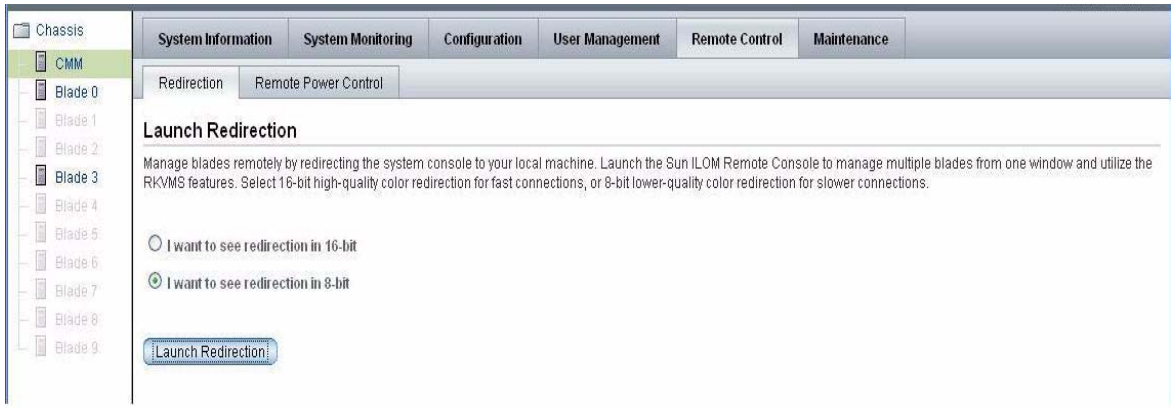
- **Bei der SP-ILOM-Webbenutzeroberfläche**. Die Seite Remote Control wird mit vier weiteren Registerkarten angezeigt: *Redirection*, *Remote Power Control*, *Mouse Mode Settings* und *Diagnostics*.

**ABBILDUNG 12-4** SP-ILOM-Registerkarte Remote Control

System Information
System Monitoring
Configuration
User Management
Remote Control
Maintenance
Redirection
Remote Power Control
Mouse Mode Settings
Diagnostics
Launch Redirection
Manage the host remotely by redirecting the system console to your local machine. Launch the Sun ILOM Remote Console to utilize the RKVMS features. Select 16-bit high-quality color redirection for fast connections, or 8-bit lower-quality color redirection for slower connections.
I want to see redirection in 16-bit
I want to see redirection in 8-bit
Launch Redirection

- **Bei der CMM-ILOM-Webbenutzeroberfläche**. Die Seite Remote Control wird mit zwei weiteren Registerkarten angezeigt: *Redirection* und *Remote Power Control*.

**ABBILDUNG 12-5** CMM-ILOM-Registerkarte Remote Control


Chassis
CMM
Blade 0
Blade 1
Blade 2
Blade 3
Blade 4
Blade 5
Blade 6
Blade 7
Blade 8
Blade 9
System Information
System Monitoring
Configuration
User Management
Remote Control
Maintenance
Redirection
Remote Power Control
Launch Redirection
Manage blades remotely by redirecting the system console to your local machine. Launch the Sun ILOM Remote Console to manage multiple blades from one window and utilize the RKVMS features. Select 16-bit high-quality color redirection for fast connections, or 8-bit lower-quality color redirection for slower connections.
I want to see redirection in 16-bit
I want to see redirection in 8-bit
Launch Redirection

---

**Hinweis –** Alternativ können Sie die Einstellungen für entfernte Steuerung für jeden Server-SP konfigurieren, der dem CMM zugeordnet ist. Für den Zugriff auf die Einstellungen für entfernte Steuerung für andere Server-SPs, die in der CMM-ILOM-Webbenutzeroberfläche aufgeführt sind, klicken Sie zuerst im linken Rahmen der Seite auf den Server-SP und dann im rechten Rahmen der Seite auf die Registerkarte Remote Control.

---

2. **Nehmen Sie auf der Seite Remote Control die folgenden Einstellungen für entfernte Steuerung vor.**

| | |
|---|---|
| Einstellungen für die Konsolenumleitung | Klicken Sie auf die Registerkarte Redirection, und wählen Sie eine der folgenden Farboptionen für die Konsolenumleitung:<br>• **8 Bit.** Wählen Sie die 8-Bit-Umleitung bei langsameren Netzwerkverbindungen.<br>• **16 Bit.** Wählen Sie die 16-Bit-Umleitung bei schnelleren Netzwerkverbindungen. |
| Mouse Mode Settings<br>*(Einstellung nur für SP)* | Klicken Sie auf die Registerkarte Mouse Mode Settings, und wählen Sie eine der folgenden Mausmoduseinstellungen:<br>• **Absolute.** Wählen Sie den Mausmodus Absolute für optimale Leistung bei Verwendung eines Betriebssystems der Familien Solaris oder Windows. Absolute ist die Standardeinstellung.<br>• **Relative.** Wählen Sie den Mausmodus Relative bei Verwendung eines Linux-Betriebssystems. Beachten Sie, dass nicht alle Linux-Betriebssysteme den Modus Absolute unterstützen. |
| Einstellungen für den Stromversorgungszustand | Klicken Sie auf die Registerkarte Remote Power Control, um einen der folgenden Stromversorgungszustände für den Hostserver auszuwählen:<br>• **Immediate Power Off.** Wählen Sie Immediate Power Off, um die Stromversorgung des entfernten Hostservers sofort auszuschalten.<br>• **Graceful Shutdown and Power Off.** Wählen Sie Graceful Shutdown and Power Off, um zu versuchen, das Betriebssystem ordnungsgemäß und ohne Fehler herunterzufahren und den entfernten Hostserver anschließend auszuschalten.<br>• **Power On**. Wählen Sie Power On, um die Stromversorgung des entfernten Hostservers vollständig einzuschalten. Power On ist die Standardeinstellung.<br>• **Power Cycle.** Wählen Sie Power Cycle, um die Stromversorgung des entfernten Hostservers sofort auszuschalten und dann dessen Stromversorgung wieder vollständig einzuschalten.<br>• **Reset.** Wählen Sie Reset, um den entfernten Hostserver sofort neu zu starten. |

| | |
|---|---|
| Einstellungen für die Konsolenumleitung | Klicken Sie auf die Registerkarte Redirection, und wählen Sie eine der folgenden Farboptionen für die Konsolenumleitung:<br>• **8 Bit.** Wählen Sie die 8-Bit-Umleitung bei langsameren Netzwerkverbindungen.<br>• **16 Bit.** Wählen Sie die 16-Bit-Umleitung bei schnelleren Netzwerkverbindungen. |
| Mouse Mode Settings<br>*(Einstellung nur für SP*) | Klicken Sie auf die Registerkarte Mouse Mode Settings, und wählen Sie eine der folgenden Mausmoduseinstellungen:<br>• **Absolute.** Wählen Sie den Mausmodus Absolute für optimale Leistung bei Verwendung eines Betriebssystems der Familien Solaris oder Windows. Absolute ist die Standardeinstellung.<br>• **Relative.** Wählen Sie den Mausmodus Relative bei Verwendung eines Linux-Betriebssystems. Beachten Sie, dass nicht alle Linux-Betriebssysteme den Modus Absolute unterstützen. |
| Einstellungen für Computerdiagnosetests<br>(*Einstellung nur für SP*)<br><br>**Hinweis:** Die Einstellungen für Computerdiagnosetests werden nur auf Systemen der Serie Sun Blade 8000 auf dem SPARC Enterprise Server nicht unterstützt. | Klicken Sie auf die Registerkarte Diagnostics, um die folgenden Einstellungen für Computerdiagnosetests zu aktivieren bzw. deaktivieren:<br>• **Disabled.** Wählen Sie Disabled, wenn beim Starten eines entfernten Hostservers keine Computerdiagnosetests ausgeführt werden sollen.<br>• **Enabled.** Wählen Sie Enabled, wenn beim Starten des entfernten Hostservers grundlegende Computerdiagnosetests ausgeführt werden sollen. Diese grundlegenden Diagnosetests dauern normalerweise 3 Minuten.<br>• **Extended.** Wählen Sie Extended, wenn beim Starten des entfernten Hostservers erweiterte Computerdiagnosetests ausgeführt werden sollen. Diese erweiterten Diagnosetests dauern normalerweise 30 Minuten. |

# Starten und Konfigurieren der ILOM-Remotekonsole für die entfernte Verwaltung von x64-Servern

Zum entfernten Verwalten eines x64-Servers müssen Sie die ILOM-Remotekonsole starten und deren Funktionen nach Bedarf für die entfernte Verwaltung konfigurieren. Weitere Informationen erhalten Sie in den folgenden Verfahren:


- „Starten der ILOM-Remotekonsole mithilfe der ILOM-Webbenutzeroberfläche“ auf Seite 220
- „Hinzufügen einer neuen Serversitzung“ auf Seite 222
- „Starten, Beenden und Neustarten der Geräteumleitung“ auf Seite 222
- „Umleiten von Tastatur- und Mausgeräten“ auf Seite 223
- „Steuern von Tastaturmodi und Sendeoptionen für Tasten“ auf Seite 224
- „Umleiten von Speichergeräten“ auf Seite 225
- „Starten, Beenden und Neustarten der Geräteumleitung“ auf Seite 222
- „Beenden der ILOM-Remotekonsole“ auf Seite 226


## ▼ Starten der ILOM-Remotekonsole mithilfe der ILOM-Webbenutzeroberfläche

**Voraussetzungen:**

- Bestehende Verbindung mit der ILOM-Webbenutzeroberfläche (SP oder CMM). Diesbezügliche Anweisungen erhalten Sie unter „Herstellen einer Verbindung mit der ILOM-Webbenutzeroberfläche“ auf Seite 215.
- Konfigurierte Einstellungen für die entfernte ILOM-Steuerung. Diesbezügliche Anweisungen erhalten Sie unter „Konfigurieren von ILOM-Einstellungen für entfernte Steuerung mithilfe der Webbenutzeroberfläche“ auf Seite 216.

Führen Sie diese Schritte durch, um die ILOM-Remotekonsole mithilfe der ILOM-Webbenutzeroberfläche zu starten:

1. **Klicken Sie in der ILOM-Webbenutzeroberfläche für einen Server-SP oder einen CMM-SP auf die Registerkarte Remote Control.**

   Die Seite Remote Console wird angezeigt.

2. **Klicken Sie auf der Seite Remote Console auf die Registerkarte Redirection.**

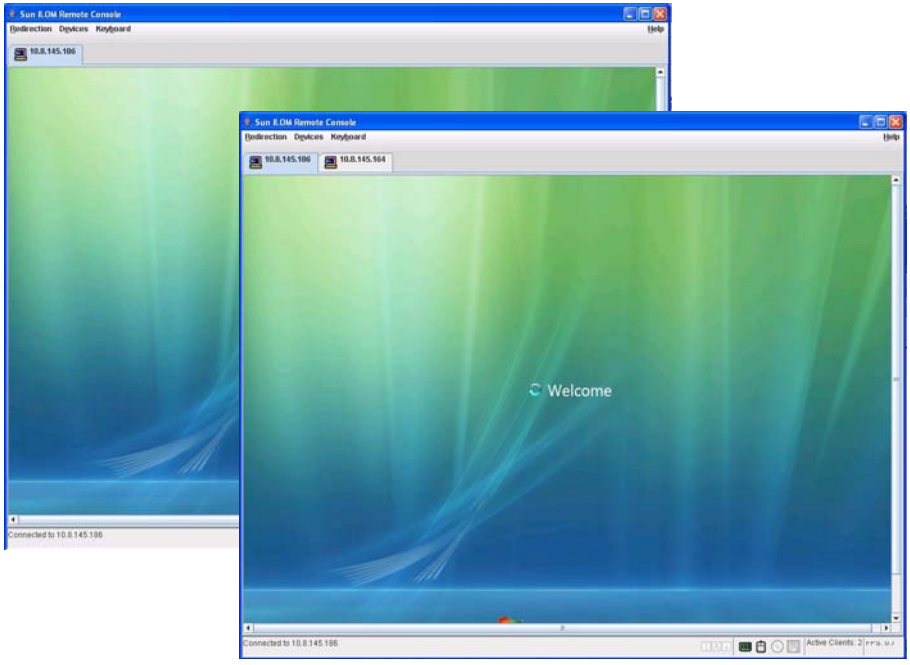
   Die Seite Redirection wird angezeigt.

3. **Klicken Sie auf der Seite Redirection auf Launch Redirection.**

   Möglicherweise wird eine Zertifikatwarnung angezeigt, die darauf hinweist, dass der Name der Site nicht mit dem Namen des Zertifikats übereinstimmt. Bei Anzeige dieser Meldung klicken Sie auf Run, um den Vorgang fortzusetzen.

   Das Fenster der ILOM-Remotekonsole wird angezeigt. Wenn eine Verbindung mit einem x64-Server-SP hergestellt wurde, wird nur eine Serversitzungs-Registerkarte angezeigt. Wenn eine Verbindung mit einem x64-CMM hergestellt wurde, können mehrere Serversitzungs-Registerkarten angezeigt werden (eine Registerkarte pro im Gehäuse installiertem Server).

**ABBILDUNG 12-6** ILOM-Remotekonsole




---

**Hinweis –** Gegebenenfalls kann die ILOM-Remotekonsole alternativ für jeden in der CMM-ILOM-Webbenutzeroberfläche aufgeführten Server-SP gestartet werden kann. Klicken Sie zum Starten der ILOM-Remotekonsole für einen einem CMM zugeordneten Server zuerst im linken Rahmen der Seite auf den Server-SP und dann auf Remote Console --> Redirection --> Launch Redirection.

---

## ▼ Hinzufügen einer neuen Serversitzung

**Voraussetzung:**

- Hergestellte Verbindung mit der ILOM-Remotekonsole. Diesbezügliche Anweisungen erhalten Sie unter „Starten der ILOM-Remotekonsole mithilfe der ILOM-Webbenutzeroberfläche“ auf Seite 220.

Führen Sie diese Schritte durch, um der ILOM-Remotekonsole eine neue Serversitzung hinzuzufügen:

1. **Wählen Sie im Fenster der ILOM-Remotekonsole Redirection --> New Session.**

   Das Dialogfeld New Session Creation wird angezeigt.

2. **Geben Sie im Dialogfeld New Session Creation die IP-Adresse eines entfernten x64-Hostserver-SP ein, und klicken Sie dann auf OK.**

   Das Anmeldedialogfeld wird angezeigt.

3. **Geben Sie im Anmeldedialogfeld den Benutzernamen mit Passwort eines Administratorkontos ein.**

   Bei den Registerkarten der ILOM-Remotekonsole wird eine Sitzungsregisterkarte für den neu hinzugefügten entfernten Hostserver angezeigt.

## ▼ Starten, Beenden und Neustarten der Geräteumleitung

**Voraussetzung:**

- Hergestellte Verbindung mit der ILOM-Remotekonsole. Diesbezügliche Anweisungen erhalten Sie unter „Starten der ILOM-Remotekonsole mithilfe der ILOM-Webbenutzeroberfläche“ auf Seite 220.

Führen Sie diese Schritte durch, um die Umleitung von Geräten zu starten, beenden oder neu zu starten:

1. **Klicken Sie im Fenster der ILOM-Remotekonsole auf das Menü Redirection.**

2. **Geben Sie im Menü Redirection gegebenenfalls die folgenden Umleitungsoptionen an:**

| | |
|---|---|
| Start Redirection | Wählen Sie Start Redirection, um die Umleitung von Geräten zu aktivieren. Start Redirection ist standardmäßig aktiviert. |
| Restart Redirection | Wählen Sie Restart Redirection, um die Umleitung von Geräten zu beenden und neu zu starten. Normalerweise wird diese Option verwendet, wenn eine gültige Umleitung immer noch aktiv ist. |
| Stop Redirection | Wählen Sie Stop Redirection, um die Umleitung von Geräten zu deaktivieren. |

In dem angezeigten Bestätigungsfenster werden Sie aufgefordert, die Änderung der Umleitungseinstellung zu bestätigen.

3. **Klicken Sie in der Bestätigungsmeldung auf Yes, um den Vorgang fortzusetzen, oder auf No, um ihn abzubrechen.**

## ▼ Umleiten von Tastatur- und Mausgeräten

**Voraussetzung:**

- Hergestellte Verbindung mit der ILOM-Remotekonsole. Diesbezügliche Anweisungen erhalten Sie unter „Starten der ILOM-Remotekonsole mithilfe der ILOM-Webbenutzeroberfläche“ auf Seite 220.

Führen Sie diese Schritte durch, um die Tastatur und Maus eines entfernten Hostservers auf Ihren lokalen Client umzuleiten:

1. **Führen Sie im Fenster der ILOM-Remotekonsole folgende Aktionen aus:**

   a. **Wählen Sie Devices --> Mouse, um die Mausumleitung zu aktivieren bzw. zu deaktivieren.**

      Die Einstellung ist standardmäßig aktiviert (Häkchen).

   b. **Wählen Sie Devices --> Keyboard, um die Tastaturumleitung zu aktivieren bzw. zu deaktivieren.**

      Die Einstellung ist standardmäßig aktiviert (Häkchen).

## ▼ Steuern von Tastaturmodi und Sendeoptionen für Tasten

**Voraussetzung:**

- Hergestellte Verbindung mit der ILOM-Remotekonsole. Diesbezügliche Anweisungen erhalten Sie unter „Starten der ILOM-Remotekonsole mithilfe der ILOM-Webbenutzeroberfläche“ auf Seite 220.

Führen Sie diese Schritte durch, um Tastaturmodi und Sendeoptionen für einzelne Tasten zu steuern:

1. **Klicken Sie im Fenster der ILOM-Remotekonsole auf das Menü Keyboard.**
2. **Nehmen Sie im Menü Keyboard gegebenenfalls die folgenden Tastatureinstellungen vor:**

| | |
|---|---|
| Auto-Keybreak Mode | Wählen Sie Auto-Keybreak Mode, um nach jedem Drücken einer Taste automatisch ein Keybreak-Signal (Lösen der Taste) zu senden. Mithilfe dieser Option können Sie Tastaturprobleme bei langsamen Netzwerkverbindungen beheben.<br>Die Auto-Keybreak-Funktion ist standardmäßig aktiviert. |
| Stateful Key Locking (Zustandsabhängige Tastenfeststellung) | Wählen Sie Stateful Key Locking, wenn der Client Stateful Key Locking verwendet (Solaris mit XSun, OSX).<br>Stateful Key Locking (Zustandsabhängige Tastenfeststellung) gilt für die folgenden drei feststellbaren Tasten: Feststelltaste (Caps Lock), Num-Feststelltaste (Num Lock) und Rollsperre (Scroll Lock). |
| Left Alt Key | Wählen Sie Left Alt Key, um die linke Alt-Taste ein-/auszuschalten. |
| Right Alt Key | Wählen Sie Right Alt Key, um bei Nicht-US-Tastaturen die rechte Alt-Taste ein-/auszuschalten.<br>Bei aktivierter Option können Sie das dritte Tastenzeichen mit einer Taste eingeben. Diese Tastaturoption bietet dieselben Funktionen wir eine AltGr-Taste. |
| F10 | Wählen Sie F10, um die F10-Funktionstaste anzuwenden (wird normalerweise im BIOS verwendet). |
| Control Alt Delete | Wählen Sie Control Alt Delete, um die Warmstartabfolge Strg-Alt-Entf zu senden. |
| Control Space | Wählen Sie Control Space, um eine Strg-Leertaste-Abfolge zu senden, um die Eingabe auf dem entfernten Host zu aktivieren. |
| Caps Lock | Wählen Sie Caps Lock, um die Feststelltaste zu senden, um die Eingabe mit russischen oder griechischen Tastaturen zu aktivieren. |

# ▼ Umleiten von Speichergeräten

**Voraussetzungen:**

- Hergestellte Verbindung mit der ILOM-Remotekonsole. Diesbezügliche Anweisungen erhalten Sie unter „Starten der ILOM-Remotekonsole mithilfe der ILOM-Webbenutzeroberfläche“ auf Seite 220.
- Bei Solaris-Clientsystemen müssen Sie vor dem Umleiten von Speichergeräten folgende Schritte durchführen:
  - Wenn Volume Manager aktiviert ist, muss diese Funktion deaktiviert werden.
  - Weisen Sie dem Prozessor, der die ILOM-Remotekonsole ausführt, rootberechtigungen zu, indem Sie folgende Befehle eingeben:

    ```
    su to root
    ppriv -s +file_dac_read pid_javarconsole
    ```
- Weitere Informationen hierzu finden Sie unter „Betriebsszenarien für die CD- und Diskettenumleitung“ auf Seite 227.

Führen Sie diese Schritte durch, um ein Speichergerät oder ein ISO-Abbild umzuleiten:

1. **Wählen Sie im Fenster der ILOM-Remotekonsole das Menü Devices.**
2. **Führen Sie im Menü Devices Folgendes aus:**
   a. **Aktivieren Sie die entsprechende Speichergerät- oder Abbildeinstellung:**

| | |
|---|---|
| CD-ROM | Wählen Sie CD-ROM, um das lokale CD-Gerät zu aktivieren. Durch diese Option verhält sich das lokale CD-ROM-Laufwerk wie ein CD-Gerät, das direkt an den entfernten Hostserver angeschlossen ist. |
| Floppy | Wählen Sie Floppy, um das lokale Diskettengerät zu aktivieren. Durch diese Option verhält sich das lokale Diskettenlaufwerk wie ein Diskettengerät, das direkt an den entfernten Hostserver angeschlossen ist. |
| CD-ROM Image | Wählen Sie CD-ROM Image, um den Speicherort eines CD-ROM-Abbilds auf dem lokalen Client oder einer Netzwerkfreigabe anzugeben. |
| Floppy Image | Wählen Sie Floppy Image, um den Speicherort eines Disketten-Abbilds auf dem lokalen Client oder einer Netzwerkfreigabe anzugeben. |

---

**Tipp –** Für die CD/DVD-Umleitung stehen nur zwei Optionen zur Auswahl. Sie können zwischen dem Umleiten eines CD-ROM-Laufwerks und dem Umleiten eines CD-ROM-Abbilds wählen.

---

**Tipp –** Bei der Installation von Software von einer Distributions-CD/DVD legen Sie die CD/DVD in das umgeleitete Laufwerk und wählen CD-ROM Drive.

**Tipp –** Bei der Installation von Software von einem ISO-Abbild legen Sie das ISO-Abbild auf dem lokalen Client oder dem freigegebenen Netzwerkdateisystem (NFS) ab und wählen dann CD-ROM Image.

In dem daraufhin angezeigten Dialogfeld werden Sie aufgefordert, die Position eines Speicherlaufwerks oder den Speicherort einer Abbilddatei anzugeben.

**b. Führen Sie zum Angeben der Speicherlaufwerkposition oder des Speicherorts der Abbilddatei eine der folgenden Aktionen aus:**

- Wählen Sie im Dialogfeld Drive Selection eine Laufwerkposition aus bzw. geben Sie diese ein, und klicken Sie auf OK.

  oder

- Wechseln Sie im Dialogfeld File Open zum Speicherort des Abbilds, und klicken Sie auf OK.

**3. Um diese Speichereinstellungen auf dem Host auch zu einem späteren Zeitpunkt erneut verwenden zu können, klicken Sie auf Devices --> Save as Host Default.**

## ▼ Beenden der ILOM-Remotekonsole

Führen Sie diese Schritte durch, um die ILOM-Remotekonsole zu beenden und alle entfernten Serversitzungen zu schließen, die eventuell noch geöffnet sind:

**1. Wählen Sie im Fenster der ILOM-Remotekonsole das Menü Redirection.**

**2. Klicken Sie im Menü Redirection auf Quit.**

# Betriebsszenarien für die CD- und Diskettenumleitung

Verwenden Sie die in TABELLE 12-2 aufgeführten Informationen, um verschiedene Fallszenarien zu bestimmen, gemäß denen sich die Umleitungsfunktion für CD- oder Diskettenlaufwerke während einer Remotekonsolensitzung verhalten könnte.

**TABELLE 12-2** Remotekonsolenbetrieb mit DVD- und Diskettenlaufwerk

| Fall | Status | DVD aus Perspektive des entfernten Hosts | Diskette aus Perspektive des entfernten Hosts |
|---|---|---|---|
| 1 | Die Remotekonsolenanwendung ist nicht gestartet, oder die Remotekonsole ist gestartet, aber die DVD-/Diskettenumleitung ist nicht gestartet. | DVD-Gerät vorhanden. Bei Abfrage durch den Host wird von ILOM keine Medienanzeige an den Host gesendet. | Diskettengerät vorhanden. Bei Abfrage durch den Host wird von ILOM keine Medienanzeige an den Host gesendet. |
| 2 | Die Remotekonsolenanwendung wurde ohne Medium im Laufwerk gestartet. | DVD-Gerät vorhanden. Bei Abfrage durch den Host, die automatisch oder bei Zugriff auf das Laufwerk auf dem Host erfolgen kann, sendet der entfernte Client eine Statusmeldung. In diesem Fall ist der Status, da kein Medium eingelegt ist, „Kein Medium“ (no medium). | Diskettengerät vorhanden. Bei Abfrage durch den Host (beispielsweise wenn Sie auf ein Laufwerk doppelklicken) sendet der entfernte Client eine Statusmeldung. In diesem Fall ist der Status, da kein Medium eingelegt ist, „Kein Medium“ (no medium). |
| 3 | Die Remotekonsolenanwendung wurde ohne Medium im Laufwerk gestartet; daraufhin wird ein Medium eingelegt. | DVD-Gerät vorhanden. Bei Abfrage durch den Host (automatisch oder manuell) sendet der entfernte Client eine Statusmeldung „Medium vorhanden“ (medium present) und zeigt ebenfalls den Medienwechsel an. | Diskettengerät vorhanden. Bei Abfrage durch den Host (manuell) sendet der entfernte Client eine Statusmeldung „Medium vorhanden“ (medium present) und zeigt ebenfalls den Medienwechsel an. |
| 4 | Die Remotekonsolenanwendung wurde mit einem Medium im Laufwerk gestartet. | Identisch mit Fall 3. | Identisch mit Fall 3. |
| 5 | Die Remotekonsolenanwendung wurde mit einem Medium im Laufwerk gestartet; daraufhin wird das Medium entnommen. | Beim nächsten Befehl vom Host wird eine Statusmeldung empfangen, die anzeigt, dass kein Medium vorhanden ist. | Beim nächsten Befehl vom Host wird eine Statusmeldung empfangen, die anzeigt, dass kein Medium vorhanden ist. |
| 6 | Die Remotekonsolenanwendung wurde mit aktivierter Abbildumleitung gestartet. | Identisch mit Fall 3. | Identisch mit Fall 3. |

**TABELLE 12-2** Remotekonsolenbetrieb mit DVD- und Diskettenlaufwerk *(Fortsetzung)*

| Fall | Status | DVD aus Perspektive des entfernten Hosts | Diskette aus Perspektive des entfernten Hosts |
|---|---|---|---|
| 7 | Die Remotekonsolenanwendung wurde mit aktiver Abbildumleitung gestartet, aber die Umleitung wurde beendet (die einzige Möglichkeit, um eine ISO-Umleitung zu beenden). | Der Treiber erkennt, dass die DVD-Umleitung beendet wurde, und sendet bei der nächsten Hostabfrage eine Statusmeldung über das fehlende Medium. | Der Treiber erkennt, dass die DVD-Umleitung beendet wurde, und sendet bei der nächsten Diskettenabfrage eine Statusmeldung über das fehlende Medium. |
| 8 | Netzwerkausfall | Die Software verfügt über einen Mechanismus zum Aufrechterhalten der Verbindung. Aufgrund ausbleibender Kommunikation erkennt sie das Versagen der Aufrechterhaltung und schließt das Socket, wobei angenommen wird, dass der Client nicht reagiert. Der Treiber sendet eine Statusmeldung „Kein Medium“ (no medium) an den Host. | Die Software verfügt über einen Mechanismus zum Aufrechterhalten der Verbindung. Sie erkennt nicht reagierende Clients und schließt das Socket. Gleichzeitig wird dem Treiber angezeigt, dass die entfernte Verbindung unterbrochen wurde. Der Treiber sendet eine Statusmeldung „Kein Medium“ (no medium) an den Host. |
| 9 | Absturz des Clients | Identisch mit Fall 8. | Identisch mit Fall 8. |

ANHANG **A**

# Referenz für die ILOM-Befehlszeilenschnittstelle (CLI)

Dieser Anhang enthält folgende Abschnitte:


- „Kurzreferenz für CLI-Befehle“ auf Seite 229
- „Referenz für CLI-Befehle“ auf Seite 235


## Kurzreferenz für CLI-Befehle

Dieser Abschnitt enthält die gängigsten ILOM-Befehle, die für die Verwaltung von Servern über die Befehlszeilenschnittstelle (CLI) verwendet werden.

**Hinweis –** In diesem Kapitel verwendete Syntaxbeispiele verwenden das Ziel beginnend mit `/SP/`. Dies könnte in Abhängigkeit von der verwendeten Serverplattform gegen das Ziel beginnend mit `/CMM/` ausgetauscht werden. Unterziele sind auf allen Serverplattformen gleich.

**TABELLE A-1** Befehl Syntax und Verwendung

| Inhalt | Schriftart | Beschreibung |
|---|---|---|
| Benutzereingabe | **`Festgelegte Breite und Fettdruck`** | Vom Benutzer einzugebender Text. Geben Sie ihn genau so ein, wie er angezeigt wird. |
| Bildschirmausgabe | `Festgelegte Breite und Normaldruck` | Vom Computer angezeigter Text. |

**TABELLE A-1** Befehl Syntax und Verwendung *(Fortsetzung)*

| Inhalt | Schriftart | Beschreibung |
|---|---|---|
| Variable | *Kursiv* | Text, der durch einen vom Benutzer zu wählenden Namen oder Wert ersetzt wird. |
| Eckige Klammern [ ] | | Text in eckigen Klammern ist optional. |
| Senkrechte Striche \| | | Durch einen senkrechten Strich getrennter Text stellt die ausschließlich verfügbaren Werte dar. Wählen Sie einen davon aus. |

**TABELLE A-2** Allgemeine Befehle

| Beschreibung | Befehl |
|---|---|
| Alle gültigen Ziele anzeigen. | **help targets** |
| Von der CLI abmelden. | **exit** |
| Die Version der auf ILOM ausgeführten ILOM-Firmware anzeigen. | **version** |
| Zeitinformationen anzeigen. | **show /SP/clock** |
| Alle CLI-Befehle anzeigen. | **show /SP/cli/commands** |
| Die aktiven ILOM-Sitzungen anzeigen. | **show /SP/sessions** |
| Informationen zu Befehlen und Zielen anzeigen. | **help** |
| Informationen zu einem bestimmten Befehl anzeigen. | **help** *create* |
| ILOM- und BIOS-Firmware aktualisieren. | **load -source** *tftp://newSPimage* |
| Eine Liste von ILOM-Ereignisprotokollen anzeigen. | **show /SP/logs/event/list** |

**TABELLE A-3** Benutzerbefehle

| Beschreibung | Befehl |
|---|---|
| Einen lokalen Benutzer hinzufügen. | **create /SP/users/***Benutzer1* **password=***Passwort* **role=administrator\|operator** |
| Einen lokalen Benutzer löschen. | **delete /SP/users/***Benutzer1* |
| Eigenschaften eines lokalen Benutzers ändern. | **set /SP/users/***Benutzer1* **role=operator** |

**TABELLE A-3** Benutzerbefehle *(Fortsetzung)*

| Beschreibung | Befehl |
|---|---|
| Informationen zu allen lokalen Benutzern anzeigen. | **show -display [**targets\|properties\|all**] -level all /SP/users** |
| Informationen zu LDAP-Einstellungen anzeigen. | **show /SP/clients/ldap** |
| LDAP-Einstellungen ändern. | **set /SP/clients/ldap binddn=***Proxybenutzer* **bindpw=***Proxybenutzerpasswort* **defaultrole=administrator\|operator ipaddress=***IPadresse* |

**TABELLE A-4** Befehle für Netzwerk- und serielle Anschlusseinstellungen

| Beschreibung | Befehl |
|---|---|
| Netzwerkkonfigurationsinformationen anzeigen. | **show /SP/network** |
| Netzwerkeigenschaften für ILOM ändern. Das Ändern bestimmter Netzwerkeigenschaften, z. B. der IP-Adresse, unterbricht die aktive Sitzung. | **set /SP/network pendingipaddress=***IPadresse* **pendingipdiscovery=dchp\|static pendingipgateway=***IPgateway* **pendingipnetmask=***IPnetzmaske* **commitpending=true** |
| Informationen zum externen seriellen Anschluss anzeigen. | **show /SP/serial/external** |
| Die Konfiguration des externen seriellen Anschlusses ändern. | **set /SP/serial/external pendingspeed=***Ganzzahl* **commitpending=true** |
| Informationen zur seriellen Verbindung mit dem Host anzeigen. | **show /SP/serial/host** |
| Die Konfiguration des seriellen Hostanschlusses ändern.<br>Hinweis: Diese Geschwindigkeitseinstellung muss mit der Geschwindigkeitseinstellung für den seriellen Anschluss 0, COM1 oder /dev/ttyS0 des Hostbetriebssystems übereinstimmen. | **set /SP/serial/host pendingspeed=***Ganzzahl* **commitpending=true** |

**TABELLE A-5** Alarmverwaltungsbefehle

| Beschreibung | Befehl |
|---|---|
| Informationen zu Alarmen anzeigen. Es können bis zu 15 Alarme konfiguriert werden. | **show /SP/alertmgmt/rules/1...15** |
| Einen IPMI PET-Alarm konfigurieren. | **set /SP/alertmgmt/rules/1...15 type=ipmipet destination=***IPadresse* **level=** down\|critical\|major\|minor |
| Einen v3 SNMP-Trap-Alarm konfigurieren. | **set /SP/alertmgmt/rules/1...15 type=snmptrap snmp_version=3 comunity_or_username=***Benutzername* **destination=***IPadresse* **level=** down\|critical\|major\|minor |
| Einen E-Mail-Alarm konfigurieren. | **set /SP/alertmgmt/rules/1...15 type=email destination=***E_Mail_Adresse* **level=** down\|critical\|major\|minor |

**TABELLE A-6** Befehle für den Zugriff auf die Systemverwaltung

| Beschreibung | Befehl |
|---|---|
| Informationen zu HTTP-Einstellungen anzeigen. | **show /SP/services/http** |
| HTTP-Einstellungen wie das Aktivieren der automatischen Umleitung auf HTTPS ändern. | **set /SP/services/http port=***Anschlussnummer* **secureredirect enabled\|disabled servicestate=**enabled\|disabled |
| Informationen zum HTTPS-Zugriff anzeigen. | **show /SP/services/https** |
| HTTPS-Einstellungen ändern. | **set /SP/services/https port=***Anschlussnummer* **servicestate=**enabled\|disabled |
| SSH DSA-Schlüsseleinstellungen anzeigen. | **show /SP/services/ssh/keys/dsa** |
| SSH RSA-Schlüsseleinstellungen anzeigen. | **show /SP/services/ssh/keys/rsa** |

**TABELLE A-7** SNMP-Befehle

| Beschreibung | Befehl |
|---|---|
| Informationen zu SNMP-Einstellungen anzeigen. Standardmäßig ist der SNMP-Anschluss „161“, und „v3“ ist aktiviert. | **show /SP/services/snmp engineid=***snmpengineid* **port=***snmpportnumber* **sets=**enabled\|disabled **v1=**enabled\|disabled **v2c=**enabled\|disabled **v3=**enabled\|disabled |
| SNMP-Benutzer anzeigen. | **show /SP/services/snmp/users** |
| Einen SNMP-Benutzer hinzufügen. | **create /SP/services/snmp/users/***snmpBenutzername* **authenticationpassword=***Passwort* **authenticationprotocol=**MD5\|SHA **permissions=**rw\|ro **privacypassword=***Passwort* **privacyprotocol=**none\|DES |
| Einen SNMP-Benutzer löschen. | **delete /SP/services/snmp/users/***snmpBenutzername* |
| Informationen zu öffentlichen (schreibgeschützten) SNMP-Communitys anzeigen. | **show /SP/services/snmp/communities/public** |
| Dieses Gerät einer öffentlichen SNMP-Community hinzufügen. | **create /SP/services/snmp/communities/ public/***comm1* |
| Dieses Gerät in einer öffentlichen SNMP-Community löschen. | **delete /SP/services/snmp/communities/ public/***comm1* |
| Informationen zu privaten (les-/schreibbaren) SNMP-Communitys anzeigen. | **show /SP/services/snmp/communities/private** |
| Dieses Gerät einer privaten SNMP-Community hinzufügen. | **create /SP/services/snmp/communities/ private/***comm2* |
| Dieses Gerät in einer privaten SNMP-Community löschen. | **delete /SP/services/snmp/communities/ private/***comm2* |

**TABELLE A-8** Hostsystembefehle

| Beschreibung | Befehl |
|---|---|
| Das Hostsystem starten oder das Gehäusenetzteil einschalten. | **start /SYS** oder **start /CH** |
| Das Hostsystem beenden oder das Gehäusenetzteil ausschalten (ordnungsgemäßes Herunterfahren). | **stop /SYS** oder **stop /CH** |
| Das Hostsystem beenden oder das Gehäusenetzteil ausschalten (erzwungenes Herunterfahren). | **stop -f /SYS** oder **stop -f /CH** |
| Das Hostsystem oder das Gehäuse zurücksetzen. | **reset /SYS** oder **reset /CH** |
| Eine Sitzung zum Herstellen einer Verbindung mit der Hostkonsole starten. | **start /SP/console** |
| Die mit der Hostkonsole verbundene Sitzung beenden (ordnungsgemäßes Herunterfahren). | **stop /SP/console** |
| Die mit der Hostkonsole verbundene Sitzung beenden (erzwungenes Herunterfahren). | **stop -force [-f] /SP/console** |

**TABELLE A-9** Befehle zum Einstellen der Zeit

| Beschreibung | Befehl |
|---|---|
| Die ILOM-Uhr für die Synchronisierung mit einem primären NTP-Server einstellen. | **set /SP/clients/ntp/server/1 address=***ntpIPadresse* |
| Die ILOM-Uhr für die Synchronisierung mit einem sekundären NTP-Server einstellen. | **set /SP/clients/ntp/server/2 address=***ntpIPadresse2* |

# Referenz für CLI-Befehle

Dieser Abschnitt enthält Referenzinformationen zu den CLI-Befehlen.

## Verwenden des Befehls `cd`

Mit dem Befehl `cd` können Sie im Namespace navigieren. Wenn Sie `cd` zu einem Zielverzeichnis ausführen, wird dieses Verzeichnis zum Standardziel für alle anderen Befehle. Bei Verwendung `-default` ohne ein Ziel wechseln Sie zur obersten Ebene des Namespace zurück. Die Eingabe von `cd -default` entspricht der Eingabe von `cd /`. Durch Eingabe von nur `cd` wird die aktuelle Position im Namespace angezeigt. Durch Eingabe von `help targets` wird eine Liste aller Ziele im gesamten Namespace angezeigt.

### Syntax

**`cd`** *Ziel*

### Optionen

**`[-default] [-h|help]`**

### Ziele und Eigenschaften

Jede Position im Namespace.

### Beispiele

Zum Erstellen eines Benutzers namens `emmett` führen Sie zuerst **`cd`** nach `/SP/users` und dann den Befehl **`create`** mit `/SP/users` als Standardziel aus.

```
-> cd /SP/users
-> create emmett
```

Um Ihre Position anzuzeigen, geben Sie **`cd`** ein.

```
-> cd /SP/users
```

## Verwenden des Befehls `create`

Mit dem Befehl `create` können Sie ein Objekt im Namespace einrichten. Wenn keine Eigenschaften zusammen mit dem Befehl `create` angegeben werden, sind diese leer.

### Syntax

**`create [`***Optionen***`] Ziel [`***Eigenschaftenname=Wert***`]`**

### Optionen

**`[-h|help]`**

### Ziele, Eigenschaften und Werte

**TABELLE A-10** Ziele, Eigenschaften und Werte für den Befehl `create`

| Gültige Ziele | Eigenschaften | Werte | Standard |
|---|---|---|---|
| **`/SP/users/`***Benutzername* | password | <Zeichenfolge> | (nicht vorhanden) |
| | role | administrator \| operator | operator |
| **`/SP/services/snmp/communities/`***communityname* | permissions | ro \| rw | ro |
| **`/SP/services/snmp/user/`***username* | authenticationprotocol | MD5 | MD5 |
| | authenticationpassword | <Zeichenfolge> | (leere Zeichenfolge) |
| | permissions | ro \| rw | ro |
| | privacyprotocol | none \| DES | DES |
| | privacypassword | <Zeichenfolge> | (leere Zeichenfolge) |

### Beispiel

```
-> create /SP/users/susan role=administrator
```

## Verwenden des Befehls `delete`

Mit dem Befehl `delete` können Sie ein Objekt aus dem Namespace entfernen. Bei der Ausführung eines `delete`-Befehls werden Sie zur Bestätigung des Vorgangs aufgefordert. Die Anzeige dieser Aufforderung können Sie durch die Verwendung der Option `-script` verhindern.

### Syntax

**`delete [`***Optionen***`] [-script]`** *Ziel*

### Optionen

**`[-f|force] [-h|help] [-script]`**

### Ziele

**TABELLE A-11** Ziele für den Befehl `delete`

| Gültige Ziele |
|---|
| **`/SP/users/`***Benutzername* |
| **`/SP/services/snmp/communities/`***communityname* |
| **`/SP/services/snmp/user/`***Benutzername* |

### Beispiele

```
-> delete /SP/users/susan
-> delete /SP/services/snmp/communities/public
```

## Verwenden des Befehls `exit`

Mit dem Befehl `exit` können Sie eine CLI-Sitzung beenden.

### Syntax

**`exit [`***Optionen***`]`**

### Optionen

**`[-h|help]`**

## Verwenden des Befehls `help`

Mit dem Befehl `help` können Sie Hilfeinformationen zu Befehlen und Zielen anzeigen. Mit der Option `-output terse` werden nur Verwendungsinformationen angezeigt. Mit der Option `-output verbose` werden Verwendungs-, Beschreibungs- und zusätzliche Informationen, einschließlich Beispielen für die Befehlsverwendung, angezeigt. Wenn die Option `-output` nicht verwendet wird, werden Verwendungsinformationen und eine kurze Beschreibung des Befehls angezeigt.

Bei Angabe von `command targets` wird eine vollständige Liste der gültigen Ziele für den Befehl aus den festen Zielen in `/SP` und `/SYS` angezeigt. Feste Ziele sind Ziele, die nicht von einem Benutzer erstellt werden können.

Bei Angabe von `command targets legal` werden Copyrightinformationen und Produktverwendungsrechte angezeigt.

### Syntax

**help [***Optionen***] command [***Ziele***]**

### Optionen

**[-h|help] [-output terse|verbose]**

### Befehle

**cd, create, delete, exit, help, load, reset, set, show, start, stop, version**

### Beispiele

- `->` **help load**

Mithilfe des Befehls `load` wird eine Datei von einem Server an ein Ziel übertragen.

Verwendung: **load -source** *URL* **[***Ziel***]**

`-source`: Gibt den Ort an, von dem eine Datei abgerufen werden soll.

- `->` **help -output verbose reset**

Mit dem Befehl `reset` wird ein Ziel zurückgesetzt.

Verwendung: **reset [-***Skript***] [***Ziel***]**

Verfügbare Optionen für diesen Befehl:

`-script`: Keine Ja/Nein-Bestätigung anfordern und so verhalten, als ob „Ja“ angegeben wäre.

Beispiel:

```
-> reset /SYS
Are you sure you want to reset /SYS (y/n)? y
Performing hard reset on /SYS
-> reset
/SP Are you sure you want to reset /SP (y/n)? n
Command aborted. ->
```

## Verwenden des Befehls `load`

Mit dem Befehl `load` können Sie eine Abbilddatei von einer Quelle, die über einen URI (Uniform Resource Indicator) angegeben ist, übertragen, um die ILOM-Firmware zu aktualisieren. Der URI kann ein Protokoll und Berechtigungsnachweise angeben, die für die Übertragung verwendet werden. Es wird nur das TFTP-Protokoll unterstützt. Daher muss der URI mit `tftp://` beginnen. Wenn Berechtigungsnachweise erforderlich, aber nicht angegeben sind, werden Sie von dem Befehl zur Eingabe eines Passworts aufgefordert. Bei Verwendung der Option `-script` entfällt die Aufforderung zur Bestätigung durch ein „Ja“ oder „Nein“ und der Befehl wird ausgeführt, als ob „Ja“ angegeben wäre.

---

**Hinweis –** Mit diesem Befehl können Sie die ILOM-Firmware und das BIOS aktualisieren.

---

### Syntax

**`load -source`** *URI*

### Optionen

**`[-h|help] [-source] [-script]`**

### Beispiel

`->` **`load -source tftp://<`***IPadresse***`>/newmainimage`**

---

**Hinweis –** Bei einem Firmware-Upgrade werden der Server und ILOM zurückgesetzt. Es wird emfpohlen, den Server vor dem Aktualisierungsverfahren ordnungsgemäß und fehlerfrei herunterzufahren. Eine Aktualisierung nimmt ungefähr fünf Minuten in Anspruch. Beim Laden einer neuen Firmware wechselt ILOM in einen speziellen Modus. Erst nach dem Abschluss des Firmware-Upgrades in ILOM und nachdem ILOM zurückgesetzt wurde, können wieder andere Aufgaben in ILOM ausgeführt werden.

---

```
 -> load -source tftp://archive/newmainimage
Are you sure you want to load the specified file (y/n)? y
File upload is complete.
Firmware image verification is complete.
Do you want to preserve the configuration (y/n)? n
Updating firmware in flash RAM:
.
Firmware update is complete.
ILOM will not be restarted with the new firmware.
```

## Verwenden des Befehls `reset`

Mit dem Befehl `reset` können Sie den Status eines Ziels zurücksetzen. Bei der Ausführung eines `reset`-Vorgangs werden Sie dessen Bestätigung aufgefordert. Die Anzeige dieser Aufforderung können Sie durch die Verwendung der Option `-script` verhindern.

---

**Hinweis –** Der Befehl `reset` wirkt sich nicht auf den Stromversorgungszustand der Hardwaregeräte aus.

---

### Syntax

**`reset [`***Optionen***`] target`**

### Optionen

**`[-h|help] [-script]`**

### Ziele

**TABELLE A-12** Ziele für den Befehl `reset`

| Gültige Ziele |
|---|
| **`/SP`** |
| **`/SYS`** |

### Beispiele

```
-> reset /SP
-> reset /SYS
```

## Verwenden des Befehls `set`

Mit dem Befehl `set` können Sie die Eigenschaften des Ziels angeben.

### Syntax

**`set [`***Optionen***`] target [`***Eigenschaftenname***`=`***Wert***`]`**

### Optionen

**`[-h|help]`**

### Ziele, Eigenschaften und Werte

**TABELLE A-13** Ziele, Eigenschaften und Werte für den Befehl `set`

| Gültige Ziele | Eigenschaften | Werte | Standard |
|---|---|---|---|
| **`/SP/users/`***Benutzername* | password | <Zeichenfolge> | (nicht vorhanden) |
| | role | administrator \| operator | operator |
| **`/SP/alertmgmt/rules`** | testalert | true | (nicht vorhanden) |
| **`/SP/alertmgmt/rules/`***Regelname* (*Regelname* = 1 bis 15) | community_or_username | <Zeichenfolge> | public |
| | destination | email_address | (nicht vorhanden) |
| | level | down \| critical \| major \| minor | (nicht vorhanden) |
| | snmp_version | 1 \| 2c \| 3 | 3 |
| | type | email \| ipmipet \| snmptrap | (nicht vorhanden) |
| **`/SP/clock`** | usentpserver | enabled \| disabled | disabled |
| | datetime | day month date time year | <Zeichenfolge> |
| **`/SP/services/http`** | port | <Ganzzahl> | 80 |
| | secureredirect | enabled \| disabled | enabled |
| | servicestate | enabled \| disabled | disabled |
| **`/SP/services/https`** | port | <Ganzzahl> | 443 |
| | servicestate | enabled \| disabled | disabled |
| **`/SP/services/snmp`** | engineid | <Hexadezimalzahl> | *IP-Adresse* |
| | port | <Ganzzahl> | 161 |
| | sets | enabled \| disabled | disabled |
| | v1 | enabled \| disabled | disabled |
| | v2c | enabled \| disabled | disabled |
| | v3 | enabled \| disabled | enabled |
| **`/SP/services/snmp/communities/private`** | permission | ro \| rw | rw |
| **`/SP/services/snmp/communities/public`** | permission | ro \| rw | ro |

**TABELLE A-13** Ziele, Eigenschaften und Werte für den Befehl `set` *(Fortsetzung)*

| Gültige Ziele | Eigenschaften | Werte | Standard |
|---|---|---|---|
| **/SP/services/snmp/user** */username* | authenticationprotocol | MD5 | MD5 |
| | authenticationpassword | <Zeichenfolge> | (leere Zeichenfolge) |
| | permissions | ro \| rw | ro |
| | privacyprotocol | none \| DES | DES |
| | privacypassword | <Zeichenfolge> | (leere Zeichenfolge) |
| **/SP/services/ssh** | generate_new_key_action | true | (nicht vorhanden) |
| | generate_new_key_type | rsa \| dsa | (nicht vorhanden) |
| | restart_sshd_action | true | (nicht vorhanden) |
| | state | enabled \| disabled | enabled |
| **/SP/services/sso** | state | | |
| **/SP/users/***Benutzername* | role | administrator \| operator | (nicht vorhanden) |
| | password | <Zeichenfolge> | (nicht vorhanden) |
| **/SP/clients/activedirectory** | state | enabled \| disabled | disabled |
| | certfilestatus | <Zeichenfolge> | (nicht vorhanden) |
| | defaultrole | <Zeichenfolge> | (nicht vorhanden) |
| | getcertfile | <Zeichenfolge> | (nicht vorhanden) |
| | ipaddress | <Zeichenfolge> | (nicht vorhanden) |
| | port | <Zeichenfolge> | (nicht vorhanden) |
| | strictcertmode | enabled \| disabled | disabled |
| | timeout | <Ganzzahl> | (nicht vorhanden) |
| | name | <Zeichenfolge> | (nicht vorhanden) |
| **/SP/clients/activedirectory/admingroups/***n* mit *n* gleich 1–5 | name | <Zeichenfolge> | (nicht vorhanden) |
| **/SP/clients/activedirectory/opergroups/***n* mit *n* gleich 1–5 | name | <Zeichenfolge> | (nicht vorhanden) |
| **/SP/clients/activedirectory/userdomains/***n* mit *n* gleich 1–5 | domain | <Zeichenfolge> | (nicht vorhanden) |
| **/SP/clients/ldap** | binddn | <username> | (nicht vorhanden) |
| | bindpw | <Zeichenfolge> | (nicht vorhanden) |
| | defaultrole | administrator \| operator | operator |
| | ipaddress | <IP-Adresse> \| none | (nicht vorhanden) |
| | port | <Ganzzahl> | 389 |
| | searchbase | <Zeichenfolge> | (nicht vorhanden) |
| | state | enabled \| disabled | disabled |

**TABELLE A-13** Ziele, Eigenschaften und Werte für den Befehl `set` *(Fortsetzung)*

| Gültige Ziele | Eigenschaften | Werte | Standard |
|---|---|---|---|
| **/SP/clients/ntp/server/[1\|2]** | address | <IP-Adresse> | (nicht vorhanden) |
| **/SP/clients/radius** | defaultrole | administrator \| operator | operator |
| | ipaddress | <IP-Adresse> \| none | (nicht vorhanden) |
| | port | <Ganzzahl> | 1812 |
| | secret | <Zeichenfolge> \| none | (nicht vorhanden) |
| | state | enabled \| disabled | disabled |
| **/SP/clients/smtp** | address | <IP-Adresse> | *IP-Adresse* |
| | port | <Ganzzahl> | 25 |
| | state | enabled \| disabled | enabled |
| **SP/clients/syslog** | destination_ip1 | <IP-Adresse> | *IP-Adresse* |
| | destination_ip2 | <IP-Adresse> | *IP-Adresse* |
| **/SP/network** | commitpending | true | (nicht vorhanden) |
| | ipaddress | <IP-Addresse> | *IP-Adresse* |
| | ipdiscovery | <IP-Addresse> | *IP-Adresse* |
| | ipgateway | <IP-Addresse> | *IP-Adresse* |
| | ipnetmask | <IP-Addresse> | *IP-Adresse* |
| | pendingipaddress | <IP-Adresse> \| none | (nicht vorhanden) |
| | pendingdiscovery | dhcp \| static | dhcp |
| | pendingipgateway | <IP-Adresse> \| none | (nicht vorhanden) |
| | pendingipnetmask | <IP in Dezimaldarstellung mit Punkten> | 255.255.255.255 |
| **/SP/serial/external** | commitpending | true | (nicht vorhanden) |
| | flowcontrol | none | none |
| | pendingspeed | <Ganzzahl aus Liste> | 9600 |
| | speed | <Ganzzahl aus Liste> | 9600 |
| **/SP/serial/host** | commitpending | true | (nicht vorhanden) |
| | pendingspeed | <Ganzzahl aus Liste> | 9600 |
| | speed | | 9600 |
| **/SP/** | system_identifier | <Zeichenfolge> | (nicht vorhanden) |
| **/SP/** | hostname | <Zeichenfolge> | abhängig von der MAC-Adresse |

### Beispiele

```
-> set /SP/users/susan role=administrator
-> set /SP/clients/ldap state=enabled binddn=proxyuser bindpw=ez24get
```

## Verwenden des Befehls `show`

Mit dem Befehl `show` können Sie Informationen zu Zielen und Eigenschaften anzeigen.

Mithilfe der Option `-display` wird der Typ der anzuzeigenden Informationen festgelegt. Wenn Sie `-display targets` angeben, werden alle Ziele im Namespace unterhalb des aktuellen Ziels angezeigt. Wenn Sie `-display properties` angeben, werden alle Eigenschaftennamen und Werte für das Ziel angezeigt. Mit dieser Option können Sie bestimmte Eigenschaftennamen angeben, um nur deren Werte anzuzeigen. Wenn Sie `-display all` angeben, werden alle Ziele im Namespace unterhalb des aktuellen Ziels sowie die Eigenschaften des angegebenen Ziels angezeigt. Wenn keine Option `-display` angegeben wird, funktioniert der Befehl `show` als ob `-display all` angegeben wäre.

Mit der Option `-level` wird die Tiefe des Befehls `show` gesteuert. Er ist für alle Modi der Option `-display` gültig. Durch Angabe von `-level 1` wird die Ebene des Namespace angezeigt, auf der das Objekt vorhanden ist. Werte größer als 1 geben Informationen zur aktuellen Ebene des Ziels im Namespace zurück sowie die <angegebener Wert> darunter liegenden Ebenen. Wenn das Argument `-level all` lautet, wird es auf die aktuelle Ebene im Namespace und alles darunter liegende angewendet.

Die Option `-o|output` gibt den Inhalt und die Form der Befehlsausgabe an. ILOM unterstützt nur `-o table`, wodurch Ziele und Eigenschaften in Tabellenform angezeigt werden.

### Syntax

**`show [options] [-display targets|properties|all] [-level`** *value*`|`**`all] target [`***Eigenschaftenname***`]`**

### Optionen

**`[-d|-display] [-l|level] [-o|output]`**

### Ziele und Eigenschaften

**TABELLE A-14** Ziele für den Befehl `show`

| Gültige Ziele | Eigenschaften |
|---|---|
| **`/SYS`** | |
| **`/SP`** | |
| **`/SP/alertmgmt/rules/`** *Regelname* (*Regelname* = 1 bis 15) | community \| username<br>destination<br>level<br>snmp_version<br>type |

**TABELLE A-14** Ziele für den Befehl `show` *(Fortsetzung)*

| Gültige Ziele | Eigenschaften |
|---|---|
| **/SP/clients/ activedirectory** | state<br>certfilestatus<br>defaultrole<br>getcertfile<br>ipaddress<br>port<br>strictcertmode<br>timeout |
| **/SP/clients/ activedirectory/ admingroups/***n*<br>mit *n* gleich 1–5 | name |
| **/SP/clients/ activedirectory/ opergroups/***n*<br>mit *n* gleich 1–5 | name |
| **/SP/clients/ activedirectory/ userdomains/***n*<br>mit *n* gleich 1–5 | domain |
| **/SP/clients/ldap** | binddn<br>bindpw<br>defaultrole<br>ipaddress<br>port<br>searchbase<br>state |
| **/SP/clients/ntp/server/[1\|2]** | ipaddress |
| **/SP/clock** | datetime<br>usentpserver |
| **/SP/logs/event** | clear |
| **/SP/network** | ipaddress<br>ipdiscovery<br>ipgateway<br>ipnetmask<br>macaddress<br>pendingipaddress<br>pendingdiscovery<br>pendingipgateway<br>pendingipnetmask |

**TABELLE A-14** Ziele für den Befehl `show` *(Fortsetzung)*

| Gültige Ziele | Eigenschaften |
|---|---|
| **/SP/serial/external** | flowcontrol<br>pendingspeed<br>speed |
| **/SP/serial/host** | pendingspeed<br>speed |
| **/SP/services/http** | port<br>secureredirect<br>servicestate |
| **/SP/services/https** | port<br>servicestate |
| **/SP/services/snmp** | engineid<br>port<br>sets<br>v1<br>v2c<br>v3 |
| **/SP/services/snmp/communities/private** | permissions |
| **/SP/services/snmp/communities/public** | permissions |
| **/SP/services/snmp/users/***Benutzername* | password<br>role |
| **/SP/services/ssh** | state |
| **/SP/services/ssh/keys/dsa** | fingerprint<br>length<br>publickey |
| **/SP/services/ssh/keys/rsa** | fingerprint<br>length<br>publickey |
| **/SP/services/sso** | state |
| **/SP/sessions** | username<br>starttime<br>date |
| **/SP/sessions/***SitzungsID* | starttime<br>source<br>type<br>user |
| **/SP/users/***Benutzername* | role<br>password |

### Beispiele

```
-> show -display properties /SP/users/susan
/SP/users/susan
Properties:
role = Administrator

-> show /SP/clients -level 2
/SP/clients
                Targets:
                                ldap
                                ntp
                Properties:
                Commands:
                                cd
                                show
/SP/clients/ldap
                Targets:
                Properties:
                                binddn = cn=Manager,dc=sun,dc=com
                                bindpw = secret
                                defaultrole = Operator
                                ipaddress = 129.144.97.180
                                port = 389
                                searchbase = ou=people,dc=sun,dc=com
                                state = disabled
                Commands:
                                cd
                                show
/SP/clients/ntp
                Targets:
                                server
                Properties:
                Commands:
                  cd
                  show
```

## Verwenden des Befehls `start`

Mit dem Befehl `start` können Sie das Ziel aktivieren oder eine Verbindung mit der Hostkonsole initiieren. Bei Verwendung der Option `-script` entfällt die Aufforderung zur Bestätigung durch ein „Ja“ oder „Nein“ und der Befehl wird ausgeführt, als ob „Ja“ angegeben wäre.

### Syntax

```
start [Optionen] Ziel
```

### Optionen

```
[-h|help] [-script]
```

### Ziele

**TABELLE A-15** Ziele für den Befehl `start`

| Gültige Ziele | Beschreibung |
|---|---|
| **`/SYS`** oder **`/CH`** | Startet das System oder Gehäuse (schaltet es ein). |
| **`/SP/console`** | Startet eine interaktive Sitzung mit dem Konsolendatenstrom. |

### Beispiele

```
-> start /SP/console
-> start /SYS
```

## Verwenden des Befehls `stop`

Mit dem Befehl `stop` können Sie das Ziel herunterfahren oder die Verbindung eines anderen Benutzers mit der Hostkonsole beenden. Bei der Ausführung eines `stop`-Befehls werden Sie zur Bestätigung des Vorgangs aufgefordert. Die Anzeige dieser Aufforderung können Sie durch die Verwendung der Option `-script` verhindern.

### Syntax

```
stop [Optionen] [-script] Ziel
```

### Optionen

```
[-f|force] [-h|help]
```

### Ziele

**TABELLE A-16** Ziele für den Befehl `stop`

| Gültige Ziele | Beschreibung |
|---|---|
| **/SYS** oder **/CH** | Fährt das angegebene System oder Gehäuse ordnungsgemäß herunter, wonach es (dessen Strom) ausgeschaltet wird. Mit der Option `-force` wird das ordnungsgemäße Herunterfahren übergangen und ein sofortiges Ausschalten erzwungen. |
| **/SP/console** | Beendet die Verbindung eines anderen Benutzers mit der Hostkonsole. |

### Beispiele

```
-> stop /SP/console
-> stop -force /SYS
```

## Verwenden des Befehls `version`

Mit dem Befehl `version` können Sie ILOM-Versionsinformationen anzeigen.

### Syntax

**version**

### Optionen

**[-h|help]**

### Beispiel

```
-> version
version SP firmware version: 1.0.0
SP firmware build number: 4415
SP firmware date: Mon Mar 28 10:39:46 EST 2005
SP filesystem version: 0.1.9
```

ANHANG **B**

# Glossar

## A

**ACL (Access Control List, Zugriffssteuerungsliste)** Ein Softwareautorisierungsmechanismus, der es ermöglicht, den Zugriff einzelner Benutzer auf einen Server zu steuern. Benutzer können ACL-Regeln definieren, die sich speziell auf eine bestimmte Datei oder ein Verzeichnis beziehen. Anhand dieser Regeln kann der Zugriff auf die Datei oder das Verzeichnis für einzelne oder mehrere Benutzer oder Gruppen gewährt oder verweigert werden.

**Administrator** Die Person, die über Vollzugriffsrechte (root) auf das verwaltete Hostsystem verfügt.

**Adresse** Im Netzwerkkontext ein eindeutiger Code, der einen Knoten im Netzwerk identifiziert. Namen wie „host1.fujitsu.com“ werden vom DNS (Domain Name Service) in vierteilige Adressen mit Punkten übersetzt, beispielsweise „168.124.3.4“.

**Adressenauflösung** Eine Methode, um Internetadressen physikalischen MAC-Adressen (Media Access Control) oder Domänenadressen zuzuordnen.

**Adressenauflösungsprotokoll (ARP)** Ein Protokoll, mit dessen Hilfe eine IP-Adresse (Internet Protocol) einer Netzwerk-Hardwareadresse (MAC-Adresse) zugeordnet wird.

**Agent** Ein Softwareprozess – normalerweise einem bestimmten lokalen, verwalteten Host entsprechend – der Verwaltungsanfragen ausführt und entfernten Benutzern lokale System- und Anwendungsinformationen zur Verfügung stellt.

**Alarm** Eine durch die Erfassung und Analyse von Fehlerereignissen erzeugte Meldung oder ein Protokoll. Ein Alarm zeigt an, dass korrektive Maßnahmen an der Hardware oder Software vorgenommen werden müssen.

**Alarmstandardformat (ASF)** Eine Preboot- oder Out-of-Band-Spezifikation für die Plattformverwaltung, die ein Gerät, wie beispielsweise einen intelligenten Ethernet-Controller, in die Lage versetzt, ASF-kompatible Sensoren der Hauptplatine autonom auf Spannungs-, Temperatur- und weitere Extremwerte zu überwachen und RMCP-Alarme (Remote Management and Control Protocol) gemäß der PET-Spezifikation (Platform Event Trap) zu senden. ASF wurde ursprünglich für Out-of-Band-Verwaltungsfunktionen von Clientdesktops entwickelt. Die Definition des ASF obliegt der DMTF (Distributed Management Task Force).

**Anschluss (Port)** Der Ort (Socket), an dem TCP/IP-Verbindungen hergestellt werden. Webserver verwenden üblicherweise Anschluss 80, FTP verwendet Anschluss 21 und Telnet verwendet Anschluss 23. Durch einen Anschluss kann ein Clientprogramm ein bestimmtes Serverprogramm auf einem Computer in einem Netzwerk angeben. Wenn ein Serverprogramm anfänglich gestartet wird, bindet es sich an die vergebene Anschlussnummer. Jeder Client, der nun diesen Server verwenden möchte, muss eine Anforderung zum Binden an diese vergebene Anschlussnummer senden.

**Anschlussnummer** Eine Nummer, die eine einzelne TCP/IP-Anwendung auf einem Hostcomputer angibt und somit ein Ziel für die Übermittlung von Daten bereitstellt.

**Authentifizierung** Der Prozess, mit dem die Identität eines Benutzers bzw. eines Geräts oder einer anderen Einheit eines Computersystems in einer Kommunikationssitzung überprüft wird, bevor der Benutzer, das Gerät oder die andere Einheit auf Systemressourcen Zugriff erhält. Sitzungsauthentifizierung kann in zwei Richtungen erfolgen. Ein Server authentifiziert einen Client, um Zugriffssteuerungsentscheidungen zu treffen. Der Client kann aber ebenfalls den Server authentifizieren. Bei SSL (Secure Sockets Layer) authentifiziert immer der Client den Server.

**Autorisierung** Der Prozess der Gewährung bestimmter Zugriffsrechte für einen Benutzer. Autorisierung basiert auf Authentifizierung und Zugriffssteuerung.

# B

**Bandbreite** Ein Maß der Informationsmenge, die über eine Kommunikationsverbindung übertragen werden kann. Hiermit wird häufig die Anzahl der Bits pro Sekunde beschrieben, die von einem Netzwerk zugestellt werden können.

**Baseboard Management Controller (BMC)** Ein Gerät, mit dem Gehäuseumgebungs-, Gehäusekonfigurations- und Gehäuseservicefunktionen verwaltet werden, und das Ereignisdaten von anderen Teilen des Systems empfängt. Die Daten werden über Sensorschnittstellen empfangen und mithilfe des Sensordatensatzes (Sensor Data Record, SDR), zu dem eine Schnittstelle bereitgestellt wird, interpretiert.

Der BMC bietet eine weitere Schnittstelle zum Systemereignisprotokoll (System Event Log, SEL). Typische Funktionen des BMC bestehen im Messen der Prozessortemperatur, der Stromversorgungswerte und der Zustände von Lüftern. Der BMC ist in der Lage, autonom Aktionen auszuführen, um die Systemintegrität zu gewährleisten.

**Baudrate** Die Rate, mit der Informationen zwischen Geräten übermittelt werden, z. B. zwischen einem Terminal und einem Server.

**Benutzeridentifizierung (Benutzer-ID)** Eine eindeutige Zeichenfolge, die einen Benutzer gegenüber einem System identifiziert.

**Benutzeridentifizierungsnummer (Benutzer-ID-Nummer)** Die jedem Benutzer, der auf ein UNIX-System zugreift, zugewiesene Nummer (UID). Das System verwendet Benutzer-ID-Nummern, um die Eigentümer von Dateien und Verzeichnissen anhand der numerischen UID zu identifizieren.

**Benutzerkonto** Ein Datensatz mit wesentlichen Benutzerinformationen, der auf dem System gespeichert ist. Jeder Benutzer, der auf ein System zugreift, verfügt über ein Benutzerkonto.

**Benutzername** Eine Kombination aus Buchstaben und eventuell Zahlen, die einen Benutzer gegenüber dem System identifiziert.

**Berechtigungen** Ein Satz von Rechten, die einem Benutzer oder einer Gruppe gewährt oder verweigert werden und die den Lese-, Schreib- und Ausführungszugriff für eine Datei oder ein Verzeichnis regeln. Bei der Zugriffssteuerung geben Berechtigungen an, ob der Zugriff auf die Verzeichnisinformationen gewährt oder verweigert wird, und sie definieren die Stufe des gewährten oder verweigerten Zugriffs.

**Binden** Im LDAP-Kontext (Lightweight Directory Access Protocol) der Authentifizierungsprozess, der von LDAP angefordert wird, wenn Benutzer auf das LDAP-Verzeichnis zugreifen. Die Authentifizierung erfolgt, wenn sich der LDAP-Client an den LDAP-Server bindet.

**BIOS (Basic Input/Output System)** Die Systemsoftware, die das Laden des Betriebssystems sowie das Testen der Hardware beim Einschalten des Systems (POST) steuert. Das BIOS ist in einem schreibgeschützten Speicherbaustein (ROM) gespeichert.

**Bits pro Sekunde (bit/s)** Die Maßeinheit für die Datenübertragungsgeschwindigkeit.

**Bootloader** Ein Programm im schreibgeschützten Speicher (ROM), das beim Einschalten des Systems automatisch ausgeführt wird, um das erste Stadium der Systeminitialisierung und Hardwaretests zu steuern (Startladeprogramm). Der Bootloader übergibt dann die Steuerung an ein komplexeres Programm, von dem das Betriebssystem geladen wird.

# C

**CA (Certificate Authority, Zertifikatsautorität)** Eine vertrauenswürdige Organisation, die öffentliche Schlüsselzertifikate herausgibt und die Identifizierung des Zertifikateigentümers bereitstellt. Eine Zertifikatsautorität für öffentliche Schlüssel gibt Zertifikate heraus, die eine Beziehung zwischen einer in dem Zertifikat benannten Einheit und einem öffentlichen Schlüssel herstellen, der zu dieser Einheit gehört und ebenfalls in dem Zertifikat enthalten ist.

**Cache** Eine Kopie von Originaldaten, die lokal gespeichert wird, häufig zusammen mit Anweisungen oder den am häufigsten verwendeten Informationen (Zwischenspeicher). Zwischengespeicherte Daten müssen bei Anforderung nicht erneut von einem entfernten Server abgerufen werden. Ein Cache erhöht die effektive Arbeitsspeichertransferrate sowie die Prozessorgeschwindigkeit.

**CLI (Befehlszeilen-schnittstelle)** Eine textbasierte Schnittstelle, die Benutzern das Eingeben ausführbarer Anweisungen an einer Befehlseingabeaufforderung ermöglicht.

**Client** Im Client/Server-Modell ein System oder eine Software in einem Netzwerk, die entfernt auf Ressourcen eines Servers im Netzwerk zugreift.

**CMM (Chassis Monitoring Module)** Ein normalerweise redundantes, während des Betrieb wechselbares Modul, das zusammen mit dem Service-Prozessor (SP) an jedem Blade ein vollständiges Gehäuseverwaltungssystem bildet.

**Coordinated Universal Time (UTC)** Das internationale Standardzeitformat (koordinierte Weltzeit). UTC wurde früher als GMT (Greenwich Meridian Time) bezeichnet. UTC wird von NTP-Servern (Network Time Protocol) zum Synchronisieren von Systemen und Geräten in einem Netzwerk verwendet.

**CRU (Customer Replaceable Unit)** Eine Systemkomponente, die vom Benutzer ohne besondere Schulung oder spezielles Werkzeug ausgetauscht werden kann.

# D

**Dateisystem** Eine konsistente Methode, mit der Informationen auf physikalischen Medien organisiert und gespeichert werden. Verschiedene Betriebssysteme haben normalerweise unterschiedliche Dateisysteme. Dateisysteme sind häufig baumähnlich strukturierte Netzwerke von Dateien und Verzeichnissen mit einem Stammverzeichnis (root) auf der obersten Ebene und über- und untergeordneten Verzeichnissen unterhalb des Stammverzeichnisses.

**DES (Data Encryption Standard)** Ein gängiger Algorithmus zum Ver- und Entschlüsseln von Daten.

**DHCP (Dynamic Host Configuration Protocol)** Ein Protokoll, das es einem DHCP-Server ermöglicht, Systemen in einem TCP/IP-Netzwerk (Transmission Control Protocol/Internet Protocol) IP-Adressen dynamisch zuzuweisen.

**Digitale Signatur** Eine Zertifizierung der Quelle digitaler Daten. Eine digitale Signatur ist eine Zahl, die von einem Kryptographieprozess mit öffentlichem Schlüssel abgeleitet wird. Wenn die Daten nach Erstellung der Signatur geändert werden, wird die Signatur ungültig. Auf diese Weise kann durch eine digitale Signatur die Datenintegrität und die Erkennung von Datenänderungen gewährleistet werden.

**Digital Signature Algorithm (DSA)** Ein durch den Digital Signature Standard (DSS) festgelegter Kryptographiealgorithmus. DSA ist ein Standardalgorithmus, der zum Erstellen digitaler Signaturen verwendet wird.

**Distinguished Name (DN)** Im LDAP-Kontext (Lightweight Directory Access Protocol) eine eindeutige Textzeichenfolge, die den Namen und die Position eines Eintrags im Verzeichnis angibt. Ein DN kann ein vollständiger Domänenname (Fully Qualified Domain Name, FQDN) sein, der den vollständigen Pfad vom Stammverzeichnis der Struktur aus enthält.

**Distributed Management Task Force (DMTF)** Ein Konsortium aus mehr als 200 Unternehmen, das Standards verfasst und fördert, die Funktionen für die entfernte Verwaltung von Computersystemen fördern sollen. Zu den Spezifikationen der DMTF zählen DMI (Desktop Management Interface), CIM (Common Information Model) und ASF (Alert Standard Format).

**DMA (Direct Memory Access)** Die direkte Übertragung von Daten in den Arbeitsspeicher ohne Überwachung durch den Prozessor.

**DMI (Desktop Management Interface)** Desktopverwaltungsschnittstelle. Eine Spezifikation, in der Standards für den Zugriff auf technische Supportinformationen zur Computerhard- und -software festgelegt sind. DMI ist unabhängig von Hardware und Betriebssystem (OS) und kann Workstations, Server sowie andere Computersysteme verwalten. Die Definition der DMI obliegt der DMTF (Distributed Management Task Force).

**Domain Name Server (DNS)** Der Server, der normalerweise Hostnamen in einer Domäne verwaltet. DNS-Server übersetzen Hostnamen wie „www.example.com“ in IP-Adressen wie „030.120.000.168“.

**Domain Name System (DNS)** Ein verteiltes System für die Namensauflösung, das Computern das Auffinden anderer Computer in einem Netzwerk oder im Internet anhand des Domänennamens ermöglicht. Das System ordnet Standard-IP-Adressen wie „00.120.000.168“ Hostnamen wie „www.fujitsu.com“ zu. Computer rufen diese Informationen normalerweise von einem DNS-Server ab.

**Domäne** Eine Gruppierung aus Hosts, die über einen Namen identifiziert wird. Die Hosts gehören normalerweise zur selben IP-Netzwerkadresse (Internet Protocol). Mit Domäne wird auch der letzte Teil eines vollständigen Domänennamens (FQDN) bezeichnet, der das Unternehmen oder die Organisation identifiziert, das bzw. die Eigentümer der Domäne ist. „fujitsu.com“ identifiziert beispielsweise Jujitsu Limited Microsystems als Eigentümer der Domäne im FQDN „docs.fujitsu.com“.

**Domänenname** Der eindeutige Name, der einem System oder einer Gruppe von Systemen im Internet zugewiesen ist. Die Hostnamen aller Systeme in der Gruppe haben dasselbe Domänennamensuffix, wie z. B. „fujitsu.com“. Domänennamen werden von rechts nach links interpretiert. „fujitsu.com“ ist beispielsweise der Domänenname von Fujitsu Limited Microsystems und eine Unterdomäne der Topleveldomäne „.com“.

# E

**Entferntes System (Remotesystem)** Ein anderes System als das, auf dem ein Benutzer arbeitet.

**EPP (Enhanced Parallel Port)** Ein Hard- und Softwarestandard, der Systemen das Übertragen von Daten mit der doppelten Geschwindigkeit von Standardparallelanschlüssen ermöglicht.

**Ereignis** Die Änderung des Zustands eines verwalteten Objekts. Das ereignisverarbeitende Subsystem kann eine Benachrichtigung senden, auf die ein Softwaresystem bei Eintreffen reagieren muss, die aber von der Software weder angefordert wurde noch von ihr gesteuert wird.

**Ethernet** Ein Industriestandardtyp für LANs (Local Area Network), der die Echtzeitkommunikation zwischen direkt über Kabel miteinander verbundenen Systemen ermöglicht. Ethernet verwendet einen CSMA/CD-Algorithmus (Carrier Sense Multiple Access/Collision Detection) als Zugriffsmethode, wobei alle Knoten prüfen, ob eine Datenübertragung stattfindet, und jeder Knoten mit der Übertragung von Daten beginnen kann. Wenn mehrere Knoten gleichzeitig mit der Übertragung beginnen („Collision"), warten die übertragenden Knoten für einen zufälligen Zeitraum, bevor ein erneuter Übertragungsversuch unternommen wird.

# F

**Failover** Die automatische Übergabe eines Computerdienstes von einem System, oder häufiger von einem Subsystem, an ein anderes zur Bereitstellung redundanter Funktionalität.

**Fast Ethernet** Ethernet-Technologie, die Daten mit bis zu 100 Megabits pro Sekunde überträgt. Fast Ethernet ist abwärtskompatibel mit Ethernet-Installationen mit 10 Megabits pro Sekunde.

**Firewall** Eine normalerweise hard- und softwareseitige Netzwerkkonfiguration, durch die vernetzte Computer innerhalb einer Organisation vor Zugriffen von außerhalb geschützt werden. Eine Firewall kann ein- und ausgehende Verbindungen von und an angegebene Dienste bzw. Hosts überwachen und verhindern.

**Firmware** Software, die normalerweise das erste Stadium des Startvorgangs eines Systems sowie die Systemverwaltung unterstützt. Die Firmware ist in einen schreibgeschützten Speicherbaustein (ROM) oder einen programmierbaren ROM (PROM) eingebettet.

**FQDN (Fully Qualified Domain Name)** Der vollständige und eindeutige Internetname eines Systems, beispielsweise „www.fujitsu.com". Der FQDN enthält einen Hostservernamen (www) sowie dessen Domänennamen der obersten Ebene (Top-Level, .com) und der zweiten Ebene (Second-Level, .fujitsu). Ein FQDN kann der IP-Adresse eines Systems zugeordnet werden.

**FRU (Field Replaceable Unit)** Eine Systemkomponente, die am Standort des Kunden ausgetauscht werden kann.

**FTP (File Transfer Protocol)** Ein grundlegendes Internetprotokoll, das auf TCP/IP (Transmission Control Protocol/Internet Protocol) basiert und das Abrufen und Speichern von Dateien zwischen Systemen über das Internet ermöglicht, unabhängig von Betriebssystem und Architektur der an der Dateiübertragung beteiligten Systeme.

# G

**Gateway** Ein Computer oder Programm, das zwei Netzwerke miteinander verbindet und zwischen den Netzwerken Datenpakete übergibt. Ein Gateway verfügt über mehr als eine Netzwerkschnittstelle.

**Geringfügiges Ereignis** Ein Systemereignis, das den Dienst zwar aktuell nicht beeinträchtigt, aber behoben werden muss, bevor es zu einer Verschlimmerung kommt.

**Gigabit Ethernet** Ethernet-Technologie, die Daten mit bis zu 1000 Megabits pro Sekunde überträgt.

**Grafische Benutzeroberfläche (GUI)** Eine Benutzeroberfläche, die grafische Elemente zusammen mit einer Tastatur und Maus verwendet, um den bequemen Zugriff auf eine Anwendung bereitzustellen.

# H

**Host** Ein System, beispielsweise ein Back-End-Server, mit einer zugewiesenen IP-Adresse und einem Hostnamen. Auf den Host wird von anderen entfernten Systemen im Netzwerk zugegriffen.

**Host-ID** Ein Teil der 32-Bit-IP-Adresse, anhand der ein Host im Netzwerk identifiziert wird.

**Hostname** Der Name eines bestimmten Computers in einer Domäne. Hostnamen sind immer einer bestimmten IP-Adresse zugeordnet.

**Hot-Plug-Funktion** Beschreibt eine Komponente, die im laufenden Betrieb eines Systems sicher entfernt oder hinzugefügt werden kann. Vor dem Entfernen der Komponente muss der Systemadministrator das System allerdings auf den Hot-Plug-Vorgang vorbereiten. Nachdem die neue Komponente eingesetzt wurde, muss der Systemadministrator das System dazu anweisen, das Gerät im System neu zu konfigurieren.

**Hot-Swap-Funktion** Beschreibt eine Komponente, die in einem laufenden System installiert oder daraus entfernt werden kann, indem sie einfach herausgenommen und eine neue eingesetzt wird. Das System erkennt den Komponentenwechsel entweder automatisch und konfiguriert sie, oder es fordert das Eingreifen des Benutzers an, um das System zu konfigurieren. Jedoch in keinem der Fälle ist ein Neustart erforderlich. Alle Hot-Swap-Komponenten verfügen über Hot-Plug-Funktionalität, aber nicht alle Hot-Plug-Komponenten verfügen über die Hot-Swap-Funktion.

**HTTP (Hypertext Transfer Protocol)** Das Internetprotokoll, mit dem Hypertextobjekte von entfernten Hosts abgerufen werden. HTTP-Nachrichten bestehen aus Anforderungen von Clients an Server sowie Antworten von Servern an Clients. HTTP basiert auf TCP/IP.

**HTTPS (Hypertext Transfer Protocol Secure)** Eine Erweiterung von HTTP, die SSL (Secure Sockets Layer) verwendet, um sichere Übermittlungen über ein TCP/IP-Netzwerk zu ermöglichen.

# I

**ICMP (Internet Control Message Protocol)** Eine Erweiterung des Internet Protocol (IP), die Funktionen für die Weiterleitung, Zuverlässigkeit, Flusssteuerung und Sequenzierung von Daten bietet. Im ICMP sind Fehler- und Steuerungsmeldungen spezifiziert, die mit dem IP verwendet werden.

**In-Band-Systemverwaltung** Eine Serververwaltungsfunktion, die nur aktiviert ist, wenn das Betriebssystem initialisiert ist und der Server ordnungsgemäß arbeitet.

**Integrated Lights Out Manager (ILOM)** Eine integrierte Hardware-, Firmware- und Softwarelösung für die In-Geräte- oder In-Blade-Systemverwaltung.

**IP (Internet Protocol)** Das Protokoll der grundlegenden Netzwerkschicht des Internet. Das IP ermöglicht die nicht zuverlässige Zustellung einzelner Pakete zwischen Hosts. IP garantiert weder, dass Pakete tatsächlich zugestellt werden, noch wie lange die Zustellung ggf. dauert oder dass mehrere Pakete in der Reihenfolge des Versendens zugestellt werden. Das IP wird durch Protokolle, die auf der IP-Schicht aufsetzen, um Verbindungszuverlässigkeit erweitert.

**IP-Adresse (Internet Protocol)** Im TCP/IP-Kontext (Transmission Control Protocol/Internet Protocol) eine eindeutige 32-Bit-Zahl, die jeden Host und jedes anderweitige Hardwaresystem in einem Netzwerk identifiziert. Die IP-Adresse ist eine durch Punkte getrennte Nummerngruppe, wie z. B. „192.168.255.256“, die die tatsächliche Position eines Computers in einem Intranet oder im Internet angibt.

**IPMItool** Ein Dienstprogramm zum Verwalten IPMI-fähiger Geräte. Mit IPMItool können IPMI-Funktionen des lokalen Systems oder eines entfernten Systems verwaltet werden. Zum Funktionsumfang gehören das Verwalten von FRU-Informationen (Field Replaceable Unit), LAN-Konfigurationen (Local Area Network) und Sensormesswerten sowie die entfernte Steuerung der Systemstromversorgung.

**IPMI (Intelligent Platform Management Interface)** Eine Schnittstellenspezifikation auf Hardwareebene, die primär für die Out-of-Band-Verwaltung von Serversystemen über eine Reihe von physikalischen Verbindungsstellen (Interconnects) entwickelt wurde. Die IPMI-Spezifikation beschreibt umfassende Abstraktionen hinsichtlich Sensoren. Hierdurch kann eine Verwaltungsanwendung, die auf dem Betriebssystem oder auf einem entfernten System ausgeführt wird, den Aufbau der Systemumgebung analysieren und sich beim IPMI-Subsystem des Systems registrieren, um so Ereignisse zu empfangen. IPMI ist kompatibel mit heterogener Verwaltungssoftware von unterschiedlichen Herstellern. Die IPMI-Funktionalität umfasst die Erstellung von FRU-Bestandsberichten (Field Replacable Unit), Systemüberwachung, Protokollierung, Systemwiederherstellung (einschließlich lokalem und entferntem Zurücksetzen des Systems sowie Ein- und Ausschaltfunktionen) und Alarme.

# J

**Java(TM) Web Start-Anwendung** Ein Startprogramm für Webanwendungen. Mit Java Web Start werden Anwendungen durch Klicken auf die Webverknüpfung gestartet. Wenn die Anwendung auf Ihrem System nicht vorhanden ist, wird sie von Java Web Start heruntergeladen und auf dem System zwischengespeichert. Nach dem Herunterladen der Anwendung in den Cache kann sie über ein Desktopsymbol oder aus dem Browser heraus gestartet werden.

# K

**KCS-Schnittstelle (Keyboard Controller Style)** Ein Schnittstellentyp, der in Tastatur-Controllern von Legacy-Computern implementiert ist. Daten werden über die KCS-Schnittstelle mithilfe eines byteweisen Handshakes übertragen.

**Kernel** Der Kern des Betriebssystems, von dem die Hardware verwaltet wird. Er stellt außerdem grundlegende Dienste wie Ablage und Ressourcenzuweisung bereit, die nicht von der Hardware zur Verfügung gestellt werden.

**Knoten** Ein adressierbarer/s Punkt bzw. Gerät in einem Netzwerk. Ein Knoten kann ein Computersystem, ein Terminal oder verschiedene Peripheriegeräte mit einem Netzwerk verbinden.

**Konsole** Ein Terminal oder dediziertes Fenster in einem Bildschirm, in dem Systemmeldungen angezeigt werden. Das Konsolenfenster ermöglicht das Konfigurieren, Überwachen und Warten zahlreicher Serversoftwarekomponenten sowie die Behebung von Problemen.

**Kritisches Ereignis** Ein Systemereignis, das den Dienst ernsthaft beeinträchtigt und sofortige Intervention erfordert.

**KVMS** Tastatur, Bildschirmanzeige, Maus und Speicher (Keyboard, Video, Mouse, Storage). Eine Reihe von Schnittstellen, durch die ein System in der Lage ist, auf Tastatur-, Bildschirm-, Maus- und Speicherereignisse zu reagieren.

# L

**LAN (Local Area Network)** Eine Gruppe von eng benachbarten Systemen, die über Verbindungshard- und -software kommunizieren können. Ethernet ist die meist eingesetzte LAN-Technologie.

**LDAP (Lightweight Directory Access Protocol)** Ein Verzeichnisdienstprotokoll, das zum Speichern, Abrufen und Verteilen von Informationen, einschließlich Benutzerprofilen, Verteilerlisten und Konfigurationsdaten, verwendet wird. LDAP wird über TCP/IP (Transmission Control Protocol/Internet Protocol) ausgeführt und funktioniert plattformübergreifend.

**LDAP-Server (Lightweight Directory Access Protocol)** Ein Softwareserver, der ein LDAP-Verzeichnis pflegt und Dienstabfragen an das Verzeichnis verarbeitet. Die Verzeichnisdienste und die Netscape-Verzeichnisdienste sind Implementierungen eines LDAP-Servers.

**Lights Out Management (LOM)** Eine Technologie, die die Funktion für die Out-of-Band-Kommunikation mit dem Server bereitstellt, auch wenn das Betriebssystem nicht ausgeführt wird. Auf diese Weise kann der Systemadministrator den Server von einem entfernten Standort aus ein- und ausschalten, Systemtemperaturen, Lüftergeschwindigkeiten usw. anzeigen und das System neu starten.

**Lokaler Host** Der Prozessor oder das System, auf dem eine Softwareanwendung ausgeführt wird.

# M

**MAC-Adresse (Media Access Control)** Weltweit eindeutige 48-Bit-Hardwareadressennummer, die in jede Netzwerk-Schnittstellenkarte (Network Interface Card, NIC) bei der Herstellung programmiert wird.

**Man Pages** UNIX-Online-Dokumentation.

**Message Digest 5 (MD5)** Eine sichere Hash-Funktion, die eine beliebige Long Data-Zeichenfolge in eine kurze Datenverarbeitung („digest“) umwandelt, die eindeutig und von fester Größe ist.

**MIB (Management Information Base)** Ein baumartig strukturiertes, hierarchisches System zum Klassifizieren von Informationen über Ressourcen in einem Netzwerk. In der MIB sind die Variablen definiert, auf die der SNMP-Master-Agent (Simple Network Management Protocol) zugreifen kann. Die MIB bietet Zugriff auf die Netzwerkkonfiguration, den Status und Statistiken des Servers. Mithilfe von SNMP können diese Informationen von einer Station zur Netzwerkverwaltung (Network Management Station, NMS) aus angezeigt werden. Aufgrund einer industrieweiten Übereinkunft werden einzelnen Entwicklern bestimmte Teile der Baumstruktur zugewiesen, denen diese dann Beschreibungen hinzufügen können, die für die jeweiligen Geräte spezifisch sind.

# N

**Namespace** In der Baumstruktur eines LDAP-Verzeichnisses (Lightweight Directory Access Protocol) ein Satz eindeutiger Namen, aus dem ein Objektname abgeleitet und eindeutig bestimmt wird. So werden beispielsweise Dateien im Datei-Namespace und Drucker im Drucker-Namespace benannt.

**Netzwerkmaske** Eine Zahl, mit deren Hilfe die Software die lokale Teilnetzadresse vom Rest einer angegebenen IP-Adresse trennt.

**Neustart** Ein Vorgang auf Betriebssystemebene, durch den ein System heruntergefahren und anschließend neu gestartet wird. Dieser Vorgang benötigt eine bestehende Stromversorgung.

**NFS (Network File System)** Ein Protokoll, das es auch sehr unterschiedlichen Hardwarekonfigurationen ermöglicht, transparent zusammenzuarbeiten.

**NIC (Network Interface Card)** Netzwerkschnittstellenkarte. Eine interne Leiterplatine oder Steckkarte, über die eine Workstation oder ein Server an ein Netzwerkgerät angeschlossen wird.

**Nicht flüchtiger Speicher** Ein Speichertyp, der sicherstellt, dass Daten auch bei einer Stromunterbrechung nicht verloren gehen.

**NIS (Network Information Service)** Ein System aus Programmen und Datendateien, mit dessen Hilfe UNIX-Systeme spezifische Informationen über Computer, Benutzer, Dateisystem und Netzwerkparameter innerhalb eines ganzen Computernetzwerks sammeln, vergleichen und gemeinsam verwenden.

**NMS (Network Management Station)** Station zur Netzwerkverwaltung. Eine leistungsfähige Workstation, auf der mindestens eine Netzwerkverwaltungsanwendung installiert ist. Die NMS wird für die entfernte Verwaltung eines Netzwerks eingesetzt.

**NTP (Network Time Protocol)** Ein Internetstandard für TCP/IP-Netzwerke. NTP synchronisiert die Uhrzeiten von Netzwerkgeräten mit Millisekundengenauigkeit mit NTP-Servern unter Verwendung der koordinierten Weltzeit (Coordinated Universal Time, UTC).

# O

**Objektkennung (OID)** Eine Zahl, die die Position eines Objekts in einer globalen Objektregistrierungsstruktur angibt. Jedem Knoten der Struktur ist eine Zahl zugewiesen. Auf diese Weise ergibt sich eine OID als Folge von Zahlen. Im Internet-Kontext werden die OID-Zahlen durch Punkte getrennt, z. B. „0.128.45.12“. Im LDAP-Kontext werden mithilfe von OIDs Schemaelemente mit ihren Objektklassen und Attributtypen eindeutig identifiziert.

**Öffentliche Schlüsselverschlüsselung (Public Key Encryption)** Eine Kryptographiemethode, die einen zweiteiligen Schlüssel (Code) verwendet, der aus einer öffentlichen und einer privaten Komponente besteht. Zum Verschlüsseln von Nachrichten werden die veröffentlichten öffentlichen Schlüssel des Empfängers verwendet. Zum Entschlüsseln von Nachrichten verwenden Empfänger ihre nicht veröffentlichten privaten Schlüssel, die nur ihnen bekannt sind. Durch die Kenntnis des öffentlichen Schlüssels können Benutzer den entsprechenden privaten Schlüssel nicht ableiten.

**OpenBoot(TM)-PROM** Eine Softwareschicht, die die Steuerung eines initialisierten Systems im Anschluss an den erfolgreichen POST (Power-on Self-Test) der Komponenten übernimmt. OpenBoot-PROM erzeugt Datenstrukturen im Arbeitsspeicher und startet das Betriebssystem.

**OpenIPMI** Eine betriebssystemunabhängige, ereignisgesteuerte Bibliothek zum Vereinfachen des Zugriffs auf die IPMI (Intelligent Platform Management Interface).

**Operator** Ein Benutzer mit eingeschränkten Rechten für das verwaltete Hostsystem.

**Out-of-Band-Systemverwaltung (OOB)** Eine Serververwaltungsfunktion, die aktiviert ist, wenn die Netzwerktreiber des Betriebssystems oder der Server nicht ordnungsgemäß arbeiten.

# P

**Parität** Eine Methode, mit der ein Computer die Übereinstimmung zwischen empfangenen und gesendeten Daten überprüft. Bezeichnet auch die zusammen mit Daten auf einem Datenträger gespeicherten Informationen, die es dem Controller ermöglichen, Daten nach einem Laufwerkfehler zu rekonstruieren.

**PEM (Privacy Enhanced Mail)** Ein Standard für Internet-E-Mail, der die Verschlüsselung von Daten zur Wahrung des Datenschutzes und der Datenintegrität vorsieht.

**Physikalische Adresse** Eine tatsächliche Hardwareadresse, die einer Speicherposition entspricht. Programme, die auf virtuelle Adressen verweisen, werden anschließend den physikalischen Adressen zugeordnet.

**Plattformereignis-Trap (PET)** Ein konfigurierter Alarm, der von einem Hardware- oder Firmware (BIOS)-Ereignis ausgelöst wird. Eine PET ist eine IPMI-spezifische (Intelligent Platform Management Interface) SNMP-Trap, die unabhängig vom Betriebssystem funktioniert.

**lattformereignisfilterung (PEF)** Ein Mechanismus, mit dem der Service-Prozessor so konfiguriert wird, dass dieser ausgewählte Aktionen ausführt, sobald Ereignismeldungen empfangen werden, z. B. das Ausschalten oder Zurücksetzen des Systems oder das Auslösen eines Alarms.

**POST (Power-On Self-Test)** Selbsttest beim Einschalten. Ein Programm, das die Komponenten der Systemhardware vor deren Initialisierung beim Systemstart untersucht und testet. POST konfiguriert verwendbare Komponenten in ein schlüssiges, initialisiertes System und übergibt dieses an den OpenBoot-PROM. POST übergibt eine Liste mit nur den Komponenten an den OpenBoot-PROM, die erfolgreich getestet wurden.

**Power Cycling** System aus- und wieder einschalten. Das Unterbrechen der Stromversorgung eines Systems mit anschließendem erneutem Einschalten.

**Protokoll** Ein Satz Regeln, der beschreibt, wie Systeme oder Geräte in einem Netzwerk Informationen austauschen.

**Proxy** Ein Mechanismus, durch den ein System im Auftrag eines anderen Systems auf Protokollanforderungen antwortet.

**PXE (Preboot Execution Environment)** Eine Industriestandard-Client/Server-Schnittstelle, mit der ein Server ein Betriebssystem über ein TCP/IP-Netzwerk mithilfe von DHCP (Dynamic Host Configuration Protocol) starten kann. Die PXE-Spezifikation beschreibt, wie die Netzwerkadapterkarte und das BIOS zusammenarbeiten, um dem primären Urladerprogramm grundlegende Netzwerkfunktionen bereitzustellen, sodass dieses in die Lage versetzt wird, ein sekundäres Bootstrapping, wie z. B. das Laden eines Betriebssystemabbilds über TFTP, über das Netzwerk durchzuführen. Auf diese Weise benötigt das primäre Urladerprogramm, wenn es gemäß PXE-Standards programmiert wurde, keine Informationen über die Netzwerkhardware des Systems.

# R

**RMCP (Remote Management and Control Protocol)** Ein Netzwerkprotokoll, durch das ein Administrator entfernt auf einen Alarm reagieren kann, indem das System ein- oder ausgeschaltet oder ein Neustart erzwungen wird.

**root** Bei UNIX-Betriebssystemen der Name des Superuser (root). Der root-Benutzer verfügt über Zugriffsberechtigungen auf alle Dateien und darf alle Vorgänge ausführen, die normalen Benutzern nicht gestattet sind. Entspricht ungefähr dem Benutzernamen „Administrator“ bei Windows Server-Betriebssystemen.

**Root-Verzeichnis (Stammverzeichnis)** Das Basisverzeichnis, von dem aus alle anderen Verzeichnisse – direkt oder indirekt – ausgehen.

**Router** Ein System, das einen Pfad zuweist, über den Netzwerkpakete und anderer Internetverkehr gesendet wird. Obwohl Hosts und Gateways auch eine Weiterleitung („Routing“) durchführen, bezeichnet der Begriff „Router“ normalerweise ein Gerät, das zwei Netzwerke miteinander verbindet.

**RPC (Remote Procedure Call)** Entfernter Prozeduraufruf. Eine Methode der Netzwerkprogrammierung, durch die ein Clientsystem Funktionen auf einem entfernten Server aufrufen kann. Der Client startet auf dem Server eine Prozedur, woraufhin das Ergebnis an den Client zurückübermittelt wird.

**RSA-Algorithmus** Ein Kryptographiealgorithmus, der von RSA Data Security, Inc, entwickelt wurde. Er kann sowohl für Verschlüsselung als auch für digitale Signaturen eingesetzt werden.

**RTC (Real-Time Clock)** Echtzeituhr. Eine batteriegestützte Komponente, die Uhrzeit und Datum eines Systems aufrechterhält, auch wenn die Stromversorgung unterbrochen ist.

# S

**Schema** Definitionen, die beschreiben, welcher Informationstyp als Einträge im Verzeichnis gespeichert werden kann. Wenn Informationen im Verzeichnis gespeichert werden, die nicht dem Schema entsprechen, können Clients, die versuchen, auf das Verzeichnis zuzugreifen, möglicherweise nicht die korrekten Ergebnisse anzeigen.

**Schwellenwert** Minimal- und Maximalwerte innerhalb eines Bereichs, die von Sensoren bei der Überwachung der Temperatur, der Spannung, der Stromstärke und der Lüftergeschwindigkeit verwendet werden.

**Schwer wiegendes Ereignis** Ein Systemereignis, das den Dienst grundsätzlich, aber nicht ernsthaft beeinträchtigt.

**SDR (Sensor Data Record)** Sensordatensatz. Um das dynamische Erkennen von Leistungsmerkmalen zu ermöglichen, umfasst die IPMI (Intelligent Platform Management Interface) diese Gruppe von Datensätzen. Hierzu gehören Softwareinformationen wie die Anzahl der vorhandenen Sensoren, deren Typ und Ereignisse sowie Schwellenwertinformationen usw. Anhand der Sensordatensätze kann die Software Sensordaten interpretieren und darstellen, ohne vorherige Informationen über die Plattform zu besitzen.

**Serielle Konsole** Ein Terminal oder eine tip-Verbindung, das/die am seriellen Anschluss des Service-Prozessors angeschlossen ist. Mithilfe einer seriellen Konsole wird das System so konfiguriert, dass weiter administrative Aufgaben ausgeführt werden können.

**Serverzertifikat** Ein Zertifikat, das mit HTTPS zum Authentifizieren von Webanwendungen verwendet wird. Das Zertifikat kann selbstsigniert oder von einer Zertifikatsautorität (CA) herausgegeben sein.

**Service-Prozessor (SP)** Ein Gerät, mit dem Gehäuseumgebungs-, Gehäusekonfigurations- und Gehäuseservicefunktionen verwaltet werden, und das Ereignisdaten von anderen Teilen des Systems empfängt. Die Daten werden über Sensorschnittstellen empfangen und mithilfe des Sensordatensatzes (Sensor Data Record, SDR), zu dem eine Schnittstelle bereitgestellt wird, interpretiert.

Der SP bietet eine weitere Schnittstelle zum Systemereignisprotokoll (System Event Log, SEL). Typische Funktionen des SP bestehen im Messen der Prozessortemperatur, der Stromversorgungswerte und der Zustände von Lüftern. Der SP ist in der Lage, autonom Aktionen auszuführen, um die Systemintegrität zu gewährleisten.

**Sitzungszeitüberschreitung.** Ein festgelegter Zeitraum, nach dem ein Server eine Benutzersitzung annullieren darf.

**SMB-Protokoll (Server Message Block).** Ein Netzwerkprotokoll, mit dem Dateien und Drucker in einem Netzwerk gemeinsam verwendet werden können. Das SMB-Protokoll bietet Clientanwendungen eine Methode zum Lesen und Schreiben in Dateien auf sowie zum Anfordern von Diensten von Serverprogrammen im Netzwerk. Mithilfe des SMB-Protokolls können Sie Dateisysteme zwischen Windows- und UNIX-Systemen einhängen. Das SMB-Protokoll wurde ursprünglich von IBM entworfen, dann aber von Microsoft Corp. modifiziert. Microsoft benannte das Protokoll in CIFS (Common Internet File System) um.

**SMTP (Simple Mail Transfer Protocol).** Ein Protokoll aus der TCP/IP-Familie, das zum Senden und Empfangen von E-Mail verwendet wird.

**SNMP (Simple Network Management Protocol).** Ein einfaches Protokoll, das für den Austausch von Daten über die Netzwerkaktivität verwendet wird. Mithilfe von SNMP werden Daten zwischen einem verwalteten Gerät und einer Station zur Netzwerkverwaltung (Network Management Station, NMS) übertragen. Bei dem verwalteten Gerät kann es sich um ein beliebiges Gerät handeln, das SNMP ausführt, wie z. B. Hosts, Router, Webserver oder andere Server im Netzwerk.

**Speicherabbilddatei (Core).** Eine vom Betriebssystem Solaris oder Linux bei Fehlfunktion und anschließender Beendigung eines Programms erstellte Datei. Das Speicherabbild („core“) enthält eine Momentaufnahme des Arbeitsspeichers zum Zeitpunkt des Auftretens des Fehlers. Wird auch als „Speicherabbilddatei bei Systemabsturz“ bezeichnet.

**SSH (Secure Shell).** Ein UNIX-Shellprogramm und -Netzwerkprotokoll, das sichere und verschlüsselte Anmeldung und Ausführung von Befehlen auf einem entfernten System über ein nicht sicheres Netzwerk ermöglicht.

**SSL (Secure Sockets Layer).** Ein Protokoll, das die Verschlüsselung der Kommunikation zwischen Client und Server in einem Netzwerk zur Wahrung des Datenschutzes ermöglicht. SSL verwendet eine Schlüsselaustauschmethode, um eine Umgebung herzustellen, in der alle ausgetauschten Daten mit einer Chiffre (Cipher) verschlüsselt und gehasht werden, um sie vor Abhören und Änderungen zu schützen. SSL stellt eine sichere Verbindung zwischen einem Webserver und einem Webclient her. HTTPS verwendet SSL.

**Superuser** Ein besonderer Benutzer, der über Rechte zum Ausführen aller administrativen Funktionen auf einem UNIX-System verfügt. Wird auch als „root“ bezeichnet.

**Systemereignisprotokoll (SEL)** Ein Protokoll, das Systemereignissen, die autonom vom Service-Prozessor oder direkt durch vom Host gesendete Ereignismeldungen protokolliert werden, nicht flüchtigen Speicher zur Verfügung stellt.

# T

**TCB (Transmission Control Block)** Der Teil von TCP/IP, der Informationen über den Zustand einer Verbindung aufzeichnet und pflegt.

**TCP/IP (Transmission Control Protocol/Internet Protocol)** Ein Internetprotokoll, das die zuverlässige Zustellung von Datenströmen zwischen Hosts bereitstellt. TCP/IP überträgt Daten zwischen verschiedenen Typen von Netzwerksystemen, wie z. B. Systemen, die Solaris-, Microsoft Windows- oder Linux-Software ausführen. TCP garantiert die Zustellung von Daten und dass Pakete in derselben Reihenfolge zugestellt werden, wie sie gesendet wurden.

**Teilnetz** Ein Arbeitsschema, das ein einziges logisches Netzwerk in kleinere physikalische Netzwerke unterteilt, um die Weiterleitung zu vereinfachen. Das Teilnetz ist der Teil einer IP-Adresse, der einen Block von Host-IDs identifiziert.

**Teilnetzmaske** Eine Bitmaske, mit der Bits aus einer Internetadresse für die Teilnetzadressierung ausgewählt werden. Die Maske ist 32 Bits lang und legt den Netzwerkteil der Internetadresse sowie mindestens ein Bit des lokalen Teils fest. Wird auch als „Adressmaske“ bezeichnet.

**Telnet** Das virtuelle Terminalprogramm, das Benutzern eines Hosts das Anmelden bei einem entfernten Host ermöglicht. Ein Telnet-Benutzer eines Hosts, der bei einem entfernten Host angemeldet ist, kann mit dem entfernten Host als normaler Terminalbenutzer interagieren.

**TFTP (Trivial File Transfer Protocol)** Ein einfaches Transportprotokoll, das Dateien an Systeme überträgt. TFTP verwendet UDP (User Datagram Protocol).

**Trap** Eine Ereignisbenachrichtigung, die von SNMP-Agenten eigenständig vorgenommen wird, wenn bestimmte Zustände oder Bedingungen erkannt werden. Im SNMP sind formal sieben Typen von Traps definiert, aber die Definition von Untertypen ist zulässig.

# U

**UDP (User Datagram Protocol)** Ein verbindungsloses Transportschichtprotokoll, das das Internet Protocol (IP) um eine gewisse Zuverlässigkeit und Multiplexing-Funktion (Mehrkanalbetrieb) erweitert. Mit UDP kann ein Anwendungsprogramm über IP Datagramme an ein anderes Anwendungsprogramm auf einem anderen Computer übermitteln. SNMP (Simple Network Management Protocol) wird normalerweise über UDP implementiert.

**Umleitung** Das Leiten einer Ein- oder Ausgabe an eine Datei oder ein Gerät statt an die Standardein- oder -ausgabe eines Systems. Als Ergebnis einer Umleitung wird die Ein- oder Ausgabe, die ein System normalerweise anzeigen würde, an den Bildschirm eines anderen Systems gesendet.

**USB (Universal Serial Bus)** Ein Standard für eine externe BUS-Architektur, der Datentransferraten von bis zu 450 Megabits pro Sekunde erlaubt (USB 2.0). Über einen USB-Anschluss werden z. B. Zeigegeräte wie Mäuse angeschlossen.

# V

**Verzeichnisserver** Im LDAP-Kontext (Lightweight Directory Access Protocol) ein Server, der Informationen über Personen und Ressourcen innerhalb einer Organisation an einem logisch zentralen Ort speichert und von dort aus bereitstellt.

# W

**WAN (Wide Area Network)** Ein Netzwerk aus vielen Systemen, das Dateiübertragungsdienste bereitstellt. Ein WAN kann einen großen physikalischen Bereich abdecken und sich manchmal sogar weltweit erstrecken.

**Webserver** Software, die Dienste für den Zugriff auf das Internet oder ein Intranet bereitstellt. Ein Webserver enthält Websites, bietet Unterstützung für HTTP/HTTPS und andere Protokolle und führt serverseitige Programme aus.

# X

**X.509-Zertifikat** Der gängigste Zertifikatstandard. X.509-Zertifikate sind Dokumente, die einen öffentlichen Schlüssel und zugeordnete Identitätsinformationen enthalten, die von einer Zertifikatsautorität (CA) digital signiert sind.

**X Window System** Ein verbreitetes UNIX-Fenstersystem, mit dem eine Workstation oder ein Terminal mehrere Sitzungen gleichzeitig steuern kann.

**XIR (Externally Initiated Reset)** Ein Signal, das einen Warmstart an den Prozessor in der Domäne sendet. XIR führt keinen Neustart der Domäne aus. Ein XIR wird im Allgemeinen verwendet, um ein hängendes System zu umgehen und an die Konsoleneingabeaufforderung zu gelangen. Der Benutzer kann dann eine Speicherauszugsdatei erzeugen, die bei der Diagnose der Ursache für das Aufhängen des Systems hilfreich sein kann.

# Z

**Zeitüberschreitung** Ein festgelegter Zeitraum, nach dem der Server aufhören soll, eine Dienstroutine abzuschließen, die zu hängen scheint.

**Zertifikat** Öffentliche Schlüsseldaten, die von einer vertrauenswürdigen Zertifikatsautorität (Certificate Authority, CA) zugewiesen wurden, um die Identität einer Einheit zu überprüfen. Es handelt sich um ein digital signiertes Dokument. Sowohl Clients als auch Server können Zertifikate haben. Wird auch als „öffentliches Schlüsselzertifikat“ bezeichnet.

**Zurücksetzen** Ein Vorgang auf Hardwareebene, durch den ein System zuerst aus- und anschließend wieder eingeschaltet wird.

# Index


## A

Abmelden von ILOM
  Mithilfe der CLI, 44
  Mithilfe der Webbenutzeroberfläche, 62
Active Directory
  Absichern durch SSL-Zertifikate, 90
  Domänen und Gruppen, 85
  Ermitteln von Benutzerautorisierungsstufen, 89
  Konfigurationseigenschaften, 84
  Konfigurieren, 83 bis 87
  Konfigurieren mithilfe der Webbenutzeroberfläche, 83
  Überblick, 82
  Verwendungszwecke, 82
Administratorkonto
  Standardbenutzername und -passwort, 66
Administrator-Rolle
  Definition, 6
  Zum Starten der Remotekonsole erforderlich, 213
Alarme
  Ändern einer Alarmregel, 146
  Angeben von Zielen, 143
  CLI-Befehle zum Verwalten von Alarmen, 150
  Deaktivieren einer Alarmregel, 147
  Definieren einer Alarmregel, 142, 145
  Erzeugen einer E-Mail-Benachrichtigung, 155
  Erzeugen von Testalarmen, 148
  Typen von Stufen, 143
  Übermitteln von SNMP-Traps, 189
  Unterstützte Typen, 142, 189
  Warnungen wegen Systemfehlern, 141
Anmelden bei ILOM
  Mithilfe der CLI, 43
  Mithilfe der Webbenutzeroberfläche, 57

## B

Baudrate, Einstellen, 174
Befehlszeilenschnittstelle (CLI)
  Abmelden von ILOM, 44
  Anmelden bei ILOM, 43
  Befehlskurzreferenz, 229 bis 234
  Befehlsreferenz, 235 bis 249
  Befehlssyntax, 40
  ILOM-Zieltypen, 38
  Überblick, 37
  Verwenden einer hierarchischen Architektur, 38
  Zugrunde liegende Spezifikation, 38
Benutzerkonten
  Administratorberechtigungen, 65
  Ändern mithilfe der CLI, 71
  Ändern mithilfe der Webbenutzeroberfläche, 77
  Angeben von Namen, 65
  Anzahl unterstützter Konten, 65
  Anzeigen einer einzelnen Sitzung mithilfe der CLI, 74
  Anzeigen einer Liste, 71
  Anzeigen eines bestimmten Kontos, 72
  Anzeigen mithilfe der CLI, 73
  Anzeigen mithilfe der Webbenutzeroberfläche, 81
  Hinzufügen mithilfe der CLI, 71
  Hinzufügen und Festlegen von Berechtigungen mithilfe der Webbenutzeroberfläche, 74
  Konfigurieren mithilfe der CLI, 72

Löschen mithilfe der CLI, 71
Löschen mithilfe der Webbenutzeroberfläche, 80
Zugewiesene Rollen, 6
Betriebssystem Solaris 10, Konfigurieren des werkseitig installierten Betriebssystems
Verwenden einer entfernten SSH-Verbindung (Secure Shell), 166
Verfahren, 153, 154, 157
Blade-Servermodule, Konfigurieren von IP-Adressen
Bearbeiten über eine Ethernet-Verbindung, 29 bis 30
Initialisieren
Über DHCP, 23 bis 25
Über statische Zuweisung, 25 bis 26
`set`, Befehl (ILOM), Tabelle der Optionen, 26

## C

CLI (Befehlszeilenschnittstelle)
Überblick, 3
CLI-Befehle
Alarmverwaltungsbefehle, 232
Allgemeine Befehle, 230
Befehle für Netzwerk und seriellen Anschluss, 231
Befehle zum Einstellen der Zeit, 234
Benutzerbefehle, 230
Hostsystembefehle, 234
SNMP-Befehle, 233
Syntax, 229
Systemzugriffsbefehle, 232
CLI-Befehlssyntax
`cd`, Befehl, 235
`create`, Befehl, 236
`delete`, Befehl, 237
`exit`, Befehl, 237
`help`, Befehl, 238
`load`, Befehl, 239
`reset`, Befehl, 240
`set`, Befehl, 241
`show`, Befehl, 244
`start`, Befehl, 248
`stop`, Befehl, 248
`version`, Befehl, 249
CMM (Chassis Monitoring Module)
Verwalten mit ILOM, 2
CMM (Chassis Monitoring Module), Konfigurieren von IP-Adressen
Bearbeiten über eine Ethernet-Verbindung, 29 bis 30
Initialisieren
Über DHCP, 24 bis 25
Über statische Zuweisung, 27 bis 28

## D

Datennetzwerk
Im Gegensatz zum Verwaltungsnetzwerk, 4, 20
DHCP (Dynamic Host Configuration Protocol)
Verwendung zum Zuweisen einer IP-Adresse, 15
Voraussetzungen für das Zuweisen von IP-Adressen, 15
Diskrete Sensoren
Ermitteln von Messwerten, 122
DNs (Distinguished Names)
Verwendung in LDAP, 96

## E

Einstellungen für Computerdiagnosetests
Konfigurieren für die Remotekonsole, 219
Einstellungen für den Stromversorgungszustand
Konfigurieren für die Remotekonsole, 218
Ereignisprotokoll
Anzeigen und Löschen mithilfe der CLI, 136
Anzeigen und Löschen mithilfe der Webbenutzeroberfläche, 134
Erfassen von Zeitstempeln, 127
Typen angezeigter Ereignisse, 126
Ethernet-Verwaltungsanschluss
Bezeichnung am Server, 13
Verbinden mit ILOM, 5, 13

## F

Fehlerverwaltung
Anzeigen von fehlerhaften Komponenten, 130 bis 131
Überwachung und Diagnose von Hardware, 129
FRUs (Field Replaceable Unit)
Ermitteln von Sensormesswerten, 120

## G

Geräteumleitung, Verhalten während einer Remotekonsolensitzung, 227

## H

Hardware
- Umleiten von Tastatur und Maus, 223

Hochladen von SSL-Zertifikaten
- Mithilfe der Webbenutzeroberfläche, 60

HTTP- oder HTTPS-Webzugriff
- Aktivieren mithilfe der CLI, 164 bis 165
- Aktivieren mithilfe der Webbenutzeroberfläche, 174 bis 175

## I

Integrated Lights Out Manager (ILOM)
- Aktualisieren der Firmware mithilfe der CLI, 205
- Aktualisieren der Firmware mithilfe der Webbenutzeroberfläche, 206 bis 207
- Anmelden mithilfe der Webbenutzeroberfläche, 57
- Anzeigen der Version mithilfe der CLI, 204
- Anzeigen der Version mithilfe der Webbenutzeroberfläche, 205
- Befehle
  - `set`, Befehl, Blades, Tabelle der Optionen, 26
- Erste Einrichtung, 12
- Herstellen einer Verbindung, 5
- Konfigurieren für die Remotekonsole, 214
- Konten zugewiesene Rollen, 6
- Leistungsmerkmale, 7
- Neue Leistungsmerkmale in 2.0, 9
- Remotekonsole, Konfigurieren und Starten, 221
- root-Kontopasswort, 66
- Schnittstellen, 3
- Systemüberwachungsfunktionen, 118
- Überblick, 1
- Umleiten von Tastatur und Maus, 223
- Vorkonfiguriertes Administratorkonto Anmelden, 66
- Zurücksetzen des SP mithilfe der Webbenutzeroberfläche, 207

Interner serieller Anschluss, 162

IP-Adresse (Internet Protocol)
- Identifizieren von über DHCP zugewiesenen Adressen, 16
- Zuweisen von statischen IP-Adressen, 18

IPMI (Intelligent Platform Management Interface)
- Baseboard Management Controller (BMC), 178
- Funktionalität, 177
- Mit ILOM kompatible Versionen, 178
- PET-Alarme (Plattformereignis-Trap), 179
- Überblick, 3, 177
- Verwenden von IPMItool, 178

IPMItool
- Beispiele für die Verwendung, 180 bis 183
- Funktionen, 178
- Referenzinformationen, 179

## L

LDAP
- Client/Server-Modell, 94
- Clientvorgänge, 95
- DNs (Distinguished Names), 96
- Konfigurieren des LDAP-Servers, 97
- Konfigurieren von ILOM für LDAP, 98 bis 99
- Überblick, 94
- Verzeichnisstruktur, 95 bis 96

## M

MAC-Adresse (Media Access Control)
- Abrufen für SP oder CMM, 16

MIB (Management Information Base)
- Beschreibung, 188
- Mit ILOM verwendete, unterstützte MIBs, 188

Mouse Mode Setting
- Konfigurieren für die Remotekonsole, 218

## N

Namespaces
- Im Zugriff von SP, 39

Netzwerkeinstellungen
- Anstehende (pending) und aktive Eigenschaften, 160
- Anzeigen mithilfe der CLI, 161
- Anzeigen mithilfe der Webbenutzeroberfläche, 170
- Konfigurieren mithilfe der CLI, 161
- Konfigurieren mithilfe der Webbenutzeroberfläche, 171 bis 172

Netzwerkverwaltungsanschluss
- Verbinden mit ILOM, 4

## O

Operator-Rolle, 6

## P

Prozess der Firmwareaktualisierung
- Überblick, 204

## R

RADIUS
- Befehle, 103 bis 105
- Client/Server-Modell, 100
- Konfigurationsparameter, 101
- Konfigurieren, 102
- Standardanschlussnummer, 105
- Überblick, 100

Remotekonsole
- Anmeldung als Administrator, 213
- Beenden der Anwendung, 226
- Einstellungen für entfernte Steuerung, 218
- Einzel- und Mehrfachansichten für Server, 211 bis 212
- Herstellen einer Verbindung mithilfe der Webbenutzeroberfläche, 215
- Hinzufügen einer neuen Serversitzung, 222
- Konfigurieren von Einstellungen für entfernte Steuerung, 216 bis 219
- Netzwerkanschlüsse und -protokolle, 213
- Starten mithilfe der Webbenutzeroberfläche, 220 bis 221
- Steuerung der Geräteumleitung, 222 bis 223
- Überblick, 3, 210
- Umleiten von Speichergeräten oder ISO-Abbildern, 225 bis 226
- Umleiten von Tastatur und Maus, 223
- Verwenden von Tastatursteuermodi, 224
- Voraussetzungen für die Installation, 213

root-Kontopasswort
- Ändern mithilfe der CLI, 69
- Ändern mithilfe der Webbenutzeroberfläche, 66

## S

Schwellenwertsensoren
- Ermitteln von Messwerten, 121

Sensormesswerte
- Ermitteln mithilfe der CLI, 121
- Ermitteln mithilfe der Webbenutzeroberfläche, 120
- Typen gemeldeter Daten, 119
- Überwachung und Diagnose von Fehlern, 129
- Unterstützte Klassen, 121

Serielle Anschlusseinstellungen
- Anstehende (pending) und aktive Eigenschaften, 163
- Anzeigen mithilfe der CLI, 163
- Anzeigen mithilfe der Webbenutzeroberfläche, 172
- Interne und externe Anschlüsse, 162
- Konfigurieren mithilfe der CLI, 163
- Konfigurieren mithilfe der Webbenutzeroberfläche, 173 bis 174
- Standardeinstellungen, 173

Serielle Hostkonsole, 162

Serielle Konsolenverbindung
- Konfigurieren der seriellen Einstellungen, 19

Serieller Anschluss, extern
- Einstellen der Baudrate, 174

Serieller Anschluss, intern
- Einstellen der Baudrate, 174

Serieller Verwaltungsanschluss
- Verbinden mit ILOM, 13

Service-Prozessor (SP)
- Verwalten mit ILOM, 2

`set`, Befehl (ILOM)
- Blade-Optionen, Tabelle, 26

Single Sign On
- Aktivieren und Deaktivieren mithilfe der CLI, 69
- Aktivieren und Deaktivieren mithilfe der Webbenutzeroberfläche, 70
- Überblick, 69
- Verwendung zum Starten der Remotekonsole, 214

SNMP (Simple Network Management Protocol)
- Funktionen von Agenten, 187
- Management Information Base (MIB), 188
- Überblick, 3, 186
- Überwachung mit Verwaltungsstationen, 187
- Unterstützte Versionen, 186
- Verwendungsbeispiele, 198 bis 201

SNMP-Benutzerkonten
- Verwalten mithilfe der CLI, 189 bis 192
- Verwalten mithilfe der Webbenutzeroberfläche, 193 bis 197
- Ziele, Eigenschaften und Werte, 191

SNMP-Traps
- Beispiel, 201
- Konfigurieren von Zielen mithilfe der CLI, 192

Konfigurieren von Zielen mithilfe der Webbenutzeroberfläche, 198
`ssh`, Befehl (Solaris)
Herstellen einer Verbinden mit einem SP, 31, 35, 136, 140, 152, 154, 155, 157, 166
SSH-Einstellungen
Schlüsselverschlüsselung mithilfe der CLI, 166
Statische IP-Adressen
Voraussetzungen für die Zuweisung, 18
System-LEDs
Aktivierungsbedingungen, 123
Anzeigen mithilfe der CLI, 125
Anzeigen mithilfe der Webbenutzeroberfläche, 124
Veränderbare Zustände, 123
Vom System zugewiesene Zustände, 124
Systemüberwachungsfunktionen
Überblick, 118

## V

Verwaltungsnetzwerk
Im Gegensatz zum Datennetzwerk, 4
Überblick, 4
Zuweisen von IP-Adressen, 20

## W

Webbenutzeroberfläche
Anmelden, 57
Configuration, Registerkarte, 51
Hochladen von SSL-Zertifikaten, 60
Komponenten, 47
Maintenance, Registerkarte, 56
Remote Control, Registerkarte, 55
Schaltflächen, 48
System Information, Registerkarte, 49
System Monitoring, Registerkarte, 50
Überblick, 3, 45
Unterstützte Browser, 46
User Management, Registerkarte, 54
Zugriffsarten, 174

## Z

Zeiteinstellungen
Festlegen mithilfe der CLI, 128
Festlegen mithilfe der Webbenutzeroberfläche, 127, 138
Zurücksetzen von ILOM
Mithilfe der Webbenutzeroberfläche, 207
Zuweisen von Netzwerkanschlüssen
Angaben für SP und CMM, 20 bis 21
Zuweisung von IP-Adressen
Bearbeiten mithilfe der CLI, 31 bis 32
Bearbeiten mithilfe der Webbenutzeroberfläche, 29 bis 30
Für einem CMM statisch zugewiesene Adressen, 27 bis 28
Für einem SP statisch zugewiesene Adressen, 25 bis 26
Für über DHCP zugewiesene Adressen, 23 bis 25

FUJITSU